**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**CỤC AN TOÀN THÔNG TIN**

**CHƯƠNG TRÌNH KHUNG “ĐÀO TẠO NGẮN HẠN VỀ AN TOÀN**

**THÔNG TIN CHO CÁN BỘ KỸ THUẬT - MỨC CƠ BẢN”**

**Nội Dung**

[Chương 1: Tổng quan về an toàn thông tin 5](#_Toc422120931)

[1.1. Khái niệm về an toàn thông tin 5](#_Toc422120932)

[1.2. Khái niệm vê đảm bảo an toàn thông tin 5](#_Toc422120933)

[1.3. Khái niệm vê đánh giá an toàn thông tin 6](#_Toc422120934)

[1.4. Những đặc tính cơ bản của thông tin cần được đảm bảo 6](#_Toc422120935)

[1.5. Giải pháp, công nghệ mới trong lĩnh vực an toàn thông tin 8](#_Toc422120936)

[1.6. Hệ thống hóa các tiêu chuẩn về an toàn thông tin. 12](#_Toc422120937)

[1.7. Tổ chức quản lý an toàn thông tin 15](#_Toc422120938)

[1.8. Mô hình, chính sách đảm bảo an toàn thông tin 18](#_Toc422120939)

[1.9. Các biện pháp đảm bảo an toàn thông tin 20](#_Toc422120940)

[Chương 2: Lỗ hổng bảo mật và các điểm yếu hệ thống 22](#_Toc422120941)

[2.1. Tổng quan về Lỗ hổng bảo mật 22](#_Toc422120942)

[2.2. Phương pháp đánh giá lỗ hổng bảo mật 23](#_Toc422120943)

[2.3. Các bước thực hiện đánh giá lỗ hổng bảo mật 25](#_Toc422120944)

[2.4. Đánh giá an toàn cho hệ thống 27](#_Toc422120945)

[2.4.1. Hệ điều hành Windows 27](#_Toc422120946)

[2.4.2. Hệ điều hành Unix/ Linux 32](#_Toc422120947)

[Chương 3: Các kỹ thuật tấn công phổ biến vào hệ thống thông tin 44](#_Toc422120948)

[3.1. Các kỹ thuật tấn công mạng điển hình 44](#_Toc422120949)

[3.2. Tấn công lớp 3 47](#_Toc422120950)

[3.3. Tấn công lớp 4 48](#_Toc422120951)

[3.4. Tấn công lớp 7 49](#_Toc422120952)

[3.5. Tấn công lớp cao 53](#_Toc422120953)

[3.6. Kỹ năng phân tích tấn công. 54](#_Toc422120954)

[Chương 4: Phần mềm mã độc 60](#_Toc422120955)

[4.1. Tổng quan phần mềm mã độc. 60](#_Toc422120956)

[4.2. Phân loại mã độc hại 61](#_Toc422120957)

[4.3. Dấu hiệu hệ thống mạng, máy tính của mình bị nhiễm mã độc hại 68](#_Toc422120958)

[4.4. Các phương pháp phân tích mã độc hại 69](#_Toc422120959)

[4.5. Xây dựng giải pháp phòng và chống phần mềm mã độc 71](#_Toc422120960)

[Chương 5: Kỹ thuật nhận dạng và ngăn chặn tấn công 75](#_Toc422120961)

[5.1. Những mối đe dọa từ không gian mạng 75](#_Toc422120962)

[5.1.1. Mối đe dọa không cấu trúc 75](#_Toc422120963)

[5.1.2. Mối đe dọa có cấu trúc 75](#_Toc422120964)

[5.1.3. Mối đe dọa từ bên ngoài 76](#_Toc422120965)

[5.1.4. Mối đe dọa từ bên trong 76](#_Toc422120966)

[5.2. Kỹ thuật phát hiện và phòng chống xâm nhập 77](#_Toc422120967)

[5.2.1. Phát hiện sự lạm dụng 77](#_Toc422120968)

[5.2.2. Phát hiện sự bất thường 78](#_Toc422120969)

[5.3. Sử dụng công nghê, kỹ thuật ngăn chặn tấn công 81](#_Toc422120970)

[5.2.1. Tường lửa 81](#_Toc422120971)

[5.2.2. Hệ thống IDS/IPS 83](#_Toc422120972)

[5.2.3. Ngăn chặn mã độc hại 85](#_Toc422120973)

[5.2.4. Mã hóa 88](#_Toc422120974)

[5.2.5. Các kỹ thuật, công nghệ khác 89](#_Toc422120975)

[Chương 6: Những vấn đề an toàn thông tin trong hệ điều hành 90](#_Toc422120976)

[6.1. Các nguyên tắc cơ bản cho an toàn hệ thống thông tin 90](#_Toc422120977)

[6.2. Một số cơ chế bảo vệ tài nguyên ở mức hệ điều hành 91](#_Toc422120978)

[6.3. Kiểm soát truy cập 95](#_Toc422120979)

[6.4. Nhận dạng/xác thực người dùng 96](#_Toc422120980)

[6.5. Nhật ký hệ thống 100](#_Toc422120981)

[6.6. Đánh giá khả năng an toàn của hệ điều hành 103](#_Toc422120982)

[6.6.1 Quét lỗ hổng 104](#_Toc422120983)

[6.6.2. Tấn công thử 106](#_Toc422120984)

[6.7. Cài đặt các bản “vá” hệ điều hành 107](#_Toc422120985)

[Chương 7: Đảm bảo an toàn ứng dụng Web, máy chủ thư điện tử 109](#_Toc422120986)

[7.1. Kiến trúc hệ thống ứng dụng web, máy chủ thư điện tử 109](#_Toc422120987)

[7.2. Các hiểm họa đối với thư tín điện tử 114](#_Toc422120988)

[7.3. Các lỗ hổng, điểm yếu thường gặp đối với ứng dụng web 122](#_Toc422120989)

[7.4. Quy trình thực hiện kiểm tra các lỗ hổng ứng dụng Web 124](#_Toc422120990)

[7.5. Các phương thức, giải pháp bảo vệ an toàn ứng dụng web 146](#_Toc422120991)

[7.6. Các phương thức, giải pháp bảo vệ, phòng chống thư rác, xác thực người gửi/nhận trên hệ thống thư điện tử 147](#_Toc422120992)

[Chương 8: Quản lý, đánh giá an toàn thông tin 149](#_Toc422120993)

[8.1. Nhu cầu và triển vọng đánh giá ATTT tại Việt nam 149](#_Toc422120994)

[8.2. Hệ thống tiêu chuẩn OWASP, ISSAF, OSSTMM 153](#_Toc422120995)

[8.2.1. Phương pháp ISSAF 153](#_Toc422120996)

[8.2.2. Phương pháp OWASP 156](#_Toc422120997)

[8.2.3. Phương pháp OSSTMM 159](#_Toc422120998)

[8.3. Thực hiện kiểm định, đánh giá hệ thống ATTT 162](#_Toc422120999)

[8.3.1. Chuẩn bị kiểm định 164](#_Toc422121000)

[8.3.2. Tạo kế hoạch kiểm định 165](#_Toc422121001)

[8.3.3. Xem xét tài liệu 165](#_Toc422121002)

[8.3.4. Kiểm tra trực tiếp 167](#_Toc422121003)

[8.3.5. Đánh giá kết quả 168](#_Toc422121004)

[8.3.6. Lập báo cáo kiểm định 169](#_Toc422121005)

[8.4. Đánh giá mức độ rủi ro thông qua kiểm định 169](#_Toc422121006)

[8.4.1. Các rủi ro xác định thông qua đánh giá 169](#_Toc422121007)

[8.4.2. Các rủi ro xác định thông qua kiểm định 170](#_Toc422121008)

[8.4.3. Phân loại rủi ro 170](#_Toc422121009)

# Tổng quan về an toàn thông tin

## Khái niệm về an toàn thông tin

Thông tin được lưu trữ bởi các sản phẩm và hệ thống CNTT là một tài nguyên quan trọng cho sự thành công của tổ chức đó, là tài sản của một cá nhân hay tổ chức. Các thông tin cá nhân lưu trữ trong hệ thống thông tin cần được giữ bí mật, bảo vệ và không bị thay đổi khi không được phép. Trong khi các sản phẩm và hệ thống CNTT 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 và trái phép, nguy cơ mất mát thông tin.

An toàn thông tin là an toàn kỹ thuật 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 mạng

## Khái niệm vê đảm bảo an toàn thông tin

Mục tiêu hướng tới của người dùng là bảo vệ các tài sản nói trên. 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.

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.

Đảm bảo an toàn thông tin 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 do nhà nước ban hành; ngăn ngừa khả năng lợi dụng mạng 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 đảm bảo an toàn thông tin bao hàm đảm bảo an toàn cho cả phần cứng và phần mềm. 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 đảm 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.

## Khái niệm vê đánh giá an toàn thông tin

Một nhu cầu thực tế đặt ra là làm thế nào để biết các sản phẩm và hệ thống có tin cậy hay không, có áp dụng các biện pháp và kỹ thuật an toàn phù hợp hay không, mức độ an toàn như thế nào? Đánh giá an toàn thông tin chính là để đáp ứng nhu cầu đó, nhằm cung cấp bằng chứng về việc đảm bảo an toàn cho các sản phẩm và hệ thống.

Mặt khác, nhiều người tiêu dùng CNTT không có đủ kiến thức, chuyên môn và tài nguyên cần thiết để phán xét về sự an toàn của các sản phẩm và hệ thống CNTT có phù hợp hay không, và cũng không thể chỉ dựa vào cam kết của các nhà phát triển. Bởi vậy, người tiêu dùng có thể nâng cao tin cậy trong các biện pháp an toàn của một sản phẩm hoặc hệ thống CNTT bằng cách đặt hàng phân tích về an toàn cho chúng, nghĩa là đánh giá an toàn.

## Những đặc tính cơ bản của thông tin cần được đảm bảo

An toàn thông tin yêu cầu nhằm đảm bảo 3 đặc điểm quan trọng nhất của thông tin, đó là: tính bí mật, tính toàn vẹn và tính sẵn sàng. Các đặc điểm này bao trùm toàn bộ phạm trù an toàn các hệ thông thông tin. Các đặc điểm này cũng đúng với mọi tổ chức, không lệ thuộc vào việc chúng chia sẻ thông tin như thế nào.

**Tính bí mật**

Tính bí mật là tâm điểm chính của mọi giải pháp an toàn cho một sản phẩm/hệ thống CNTT. 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 đựợc phép vào các khu vực là độc quyền của các cá nhân, tổ chức.

**Tính toàn vẹn**

Tính toàn vẹn, không bị sửa đổi là đặc tính phức hợp nhất và dễ bị hiểu lầm của thông tin. Một định nghĩa khái quát hơn được sử dung ở trong tài liệu này là vấn đề cấp độ là chất lượng của số liệu (thông tin), chứ không phải là con người được/ hoặc không được phép truy cập. Đặc tính toàn vẹn được hiểu là chất lượng của thông tin được xác định căn cứ vào độ xác thực 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 môt loạt các 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**

Tính sẵn sàng của thông tin cũng là một đặc tính quan trọng, không khác gì các đặc tính đã đề cập đến ở. 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.

## Giải pháp, công nghệ mới trong lĩnh vực an toàn thông tin

**Tường lửa thế hệ mới**

Tường lửa là giải pháp được sử dụng nhiều trong các tổ chức hiện nay để ngăn chặn các cuộc tấn công từ không gian mạng, tuy nhiên phần lớn các loại tường lửa thường không đủ thông minh để có thể đọc hiểu từng loại thông tin và phân tích nội dung nó tốt hay xấu. Chính vì vậy việc tưởng lửa thế hế mới là đòi hỏi cần thiết để đáp ứng sự phát triển của ngành. Một tường thế hệ mới có thể kiểm tra ứng dụng cho phép tổ chức có thể quản lý những mối nguy hiểm uyển chuyển hơn nhiều. Những yếu tố quan trọng trong Firewall thế hệ mời bao gồm khả năng sau:

• Nhận dạng những ứng dụng hoạt động trên tất cả các cổng bất chấp giao thức nào, phương thức mã hóa hay lẩn tránh.

• Kích hoạt chính sách kiểm soát dựa trên nhận dạng người dùng hoặc nhóm người dùng chứ không chỉ kiểm tra địa chỉ IP.

• Bảo vệ hệ thống ở chế độ thời gian thực chống lại các cuộc tấn công và những phần mềm nguy hại được nhúng vào những ứng dụng.

• Đơn giản hóa chính sách quản lý với công cụ ảo hóa mạnh mẽ và quản lý chính sách hiệu quả.

• Cho phép lưu lượng băng thông hàng gigabit mà không bị giảm thiểu hiệu năng khi triển khai.

**Công nghệ tất cả trong một – UTM**

UTM (Unified Threat Management) được đề cập nhiều trong những năm gần đây. Đó là một giải pháp quản lý thống nhất và được thiết kế theo phương châm “tất cả trong một”, tích hợp các chức năng an toàn thông tin cơ bản trong cùng một thiết bị như: Tường lửa/mạng riêng ảo (VPN); phát hiện và ngăn chặn tấn công xâm nhập (IPS/IDS); nhúng chức năng phòng chống virus và lọc, kiểm soát nội dung truy cập Web. UTM có nhiều ưu điểm như chi phí đầu tư thấp, quản trị đơn giản, các thành phần bảo mật đơn lẻ được cấu hình trong cùng một giao diện và có thể tương tác với nhau một cách thông suốt trong môi trường quản trị thống nhất.

Có thể phân chia các sản phẩm UTM thành hai dòng. Dòng thứ nhất bao gồm những sản phẩm được thiết kế trên cơ sở tích hợp thiết bị của cùng một hãng sản xuất. Cách tiếp cận này tiện lợi cho nhà sản xuất nhưng với người dùng có thể là rủi ro bởi phải “phó thác” độ an toàn cho một nhà sản xuất. Dòng thứ hai được xây dựng trên quan điểm của hãng CrossBeam, theo đó UTM được thiết kế trên cơ sở sử dụng sản phẩm bảo mật của các hãng tốt nhất như: Check Point về tường lửa; Trend Micro về phòng chống virus; Websense về lọc Web; Imperva về tường lửa bảo vệ CSDL, tường lửa ứng dụng Web; ISS, Sourcefire về chống tấn công, ngăn chặn xâm nhập.... Chúng được quản lý và tích hợp trong cùng một thiết bị chuyên dụng của CrossBeam. Theo đánh giá của nhiều chuyên gia, UTM của Crossbeam có một số ưu thế: công nghệ tiên tiến, dễ quản trị, kiến trúc an ninh đơn giản, dễ cài đặt mở rộng, chi phí thấp.

**Hệ thống phát hiện và chống xâm nhập phối hợp – CIDS**

UTM phù hợp với những tổ chức vừa và nhỏ, có mạng liên lạc được bố trí tập trung trên một mặt bằng địa lý, nhưng không phù hợp với những mạng diện rộng, được bố trí trên nhiều vùng khác nhau, tương ứng mỗi vùng lại có hệ thống cảnh báo và chống xâm nhập riêng. Với những mạng loại này, người ta sử dụng giải pháp dùng một thiết bị kết nối với các thiết bị đơn lẻ tạo thành một hệ thống có khả năng bao quát toàn mạng, xử lý thông tin tổng thể và có khả năng hướng dẫn hoặc đưa ra lệnh hành động cho các khu vực đơn lẻ. Giải pháp này được gọi là hệ thống phối hợp phát hiện và chống xâm nhập (Collaborative Intrusion Detection System - CIDS).

Về kiến trúc, CIDS bao gồm hai thành phần chính: Khối xử lý thông tin (Correlation Unit) đóng vai trò trung tâm của CIDS và các khối phát hiện (Detection Unit). Các khối phát hiện thực chất là các thiết bị IDPS, Firewall có chức năng bảo vệ các vùng mạng riêng biệt, phát hiện và ngăn chặn các truy cập trái phép từ bên ngoài vào hệ thống nội bộ. Khối xử lý thông tin kết nối với các khối phát hiện qua các sensor. Một trong những khó khăn khi xây dựng hệ thống CIDS là các khối phát hiện sử dụng các công cụ bảo vệ khác nhau, ví dụ khối phát hiện này sử dụng Snort, nhưng khối khác lại sử dụng Firewall IPtable. Vấn đề này được giải quyết bằng cách: khối phát hiện dùng công cụ phát hiện xâm nhập nào, thì sensor tương ứng sẽ chạy công cụ tương tự như thế trong hệ thống, các công cụ này được gọi là các Plugin. Như vậy, trên khối xử lý thông tin sẽ chạy nhiều Plugin khác nhau, tương tự với các công cụ an toàn thông tin trên khối phát hiện.

Với cấu trúc thiết kế nói trên, CIDS có khả năng kiểm soát toàn bộ các tấn công cùng lúc xuất hiện từ nhiều hướng khác nhau, do đó có triển vọng rất lớn trong đảm bảo an toàn mạng diện rộng. Có thể thấy rõ lợi ích của CIDS so với các thiết bị đơn lẻ qua ví dụ sau: Khi một kẻ tấn công vào mạng, chúng dò tìm mật khẩu với các user mặc định đã có sẵn trong hệ thống. Với nguyên tắc không được thử mật khẩu ba lần, kẻ tấn công sẽ chỉ thử hai lần, nếu không thành công chúng chuyển sang máy khác. Bằng cách như vậy, chúng có thể dò tìm mật khẩu của mỗi tài khoản nhiều lần mà không bị phát hiện. Song đối với CIDS thì điều này không thể xảy ra, vì mỗi sự kiện trên mạng đều được gửi về trung tâm, người quản trị do đó nhận thấy có sự tìm kiếm mật khẩu nhiều lần ở nhiều máy tính khác nhau, sẽ khóa tài khoản nghi ngờ đang tìm cách truy cập vào hệ thống, hoặc đưa ra những quyết định cần thiết.

Mô hình của các hệ thống CIDS đã được nghiên cứu trong nhiều năm qua và một số sản phẩm đã được ứng dụng trong thực tế. Trong số các hệ thống CIDS được xây dựng dựa trên mã nguồn mở, nổi bật là Hệ thống quản lý an toàn thông tin OSSIM (Open Source Security Information Management). Đây không chỉ là một hệ thống CIDS đơn thuần mà nó còn cho phép quản lý ở mức rộng hơn, tới các yếu tố có liên quan đến an toàn thông tin. Về phát hiện và ngăn chặn xâm nhập, hệ thống OSSIM cho phép một máy chủ quản lý nhiều máy trạm làm nhiệm vụ thu thập dữ liệu, tiếp nhận các sự kiện gửi về, phân tích dựa trên các tập luật và đưa ra các cảnh báo cùng hành động đáp trả dựa trên cấu hình đã được xác định trước. Một số hệ thống CIDS được xây dựng thành các sản phẩm thương mại hóa như hệ thống ISS (Internet Security System) của IBM, Checkpoint Endpoint Security của hãng Checkpoint,...

**Công nghệ big data**

Trong những năm gần đây xu thế tấn công trên không gian mạng ngày gia tăng, các công nghệ như tường lửa, hệ thống SIEM, hệ thống phát hiện và ngăn chặn xâm nhập… đã góp phần đáng kể trong việc gia tăng khả năng phòng thủ cho hệ thống của các tổ chức, tuy nhiên với sự phát triển của công nghệ, truyền thông thì lượng dữ liệu sinh ra mỗi ngày trong các tổ chức là rất lớn. Chính vì thế sự xuất hiện của Big Data (Dữ liệu lớn) như một xu thế tất yếu, việc kết hợp Big Data với các giải pháp bảo mật đã có trước đó đã mở ra một hướng tiếp cận mới trong việc nghiên cứu và phát triển các giải pháp đảm bảo an toàn thông tin.

Việc phân tích các bản ghi dữ liệu sinh ra từ các thiết bị mạng, các ứng dụng, các gói tin mạng và các sự kiện hệ thống phục vụ cho mục đích điều tra và phát hiện xâm nhập vốn là một trong những vấn đề quan trọng trong an ninh thông tin từ trước đến nay, tuy nhiên, các công nghệ truyền thống thất bại trong việc cung cấp các công cụ phân tích dài hạn, quy mô lớn vì những lý do như việc lưu trữ và giữ lại một số lượng lớn dữ liệu là không khả thi về mặt kinh tế. Kết quả là, hầu hết các bản ghi nhật ký sự kiện trên các hệ thống, thiết bị thường được xóa sau một thời gian duy trì cố định. Sự ra đời của các công nghệ Big Data mới, như các cơ sở dữ liệu liên quan tới hệ sinh thái Hadoop và xử lý dòng, cho phép lưu trữ và phân tích các tập dữ liệu không đồng nhất lớn ở quy mô và tốc độ chưa từng có. Những công nghệ này sẽ chuyển đổi phân tích an ninh bằng cách thu thập dữ liệu ở một quy mô lớn từ nhiều nguồn từ các bản ghi nhật ký hệ thống, ứng dụng đến các cơ sở dữ liệu về lỗ hổng bảo mật, dữ liệu về tấn công mạng, dữ liệu mã độc… Cùng với đó là việc thực hiện phân tích sâu hơn trên dữ liệu đã có, cung cấp một cái nhìn hợp nhất các thông tin liên quan đến an ninh và đảm bảo được việc phân tích thực hiện theo thời gian thực luồng dữ liệu. Chính vì thế Big Data được ứng dụng nhiều điều trong các nghiên cứu về an toàn thông tin trên thế giới:

## Hệ thống hóa các tiêu chuẩn về an toàn thông tin.

**ISO/IEC 27002:2005 (Bộ luật thực thi về quản lý an toàn thông tin)**

Đây là tiêu chuẩn quốc tế được đưa ra bởi Viện Tiêu chuẩn Anh quốc (BSI), là một bộ quy định thực thi về quản lý an toàn thông tin và được coi như là hướng dẫn cơ bản chung, có thể phát triển thành các tiêu chuẩn an toàn thông tin và quản lý hiệu quả hoạt động của tổ chức. Tiêu chuẩn này bao gồm các hướng dẫn và các khuyến nghị về các trường hợp triển khai cho 10 lĩnh vực về an toàn thông tin bao gồm: Chính sách an toàn; Tổ chức thực hiện an toàn thông tin; Quản lý đánh giá; An toàn nguồn nhân lực; An toàn môi trường và vật lý; quản lý vận hành và giao tiếp; điều kiện truy nhập; duy trì, phát triển và thu thập thông tin; quản lý các vụ việc về an toàn thông tin; quản lý tính liên tục trong hoạt động sản xuất, kinh doanh; và tính tương thích. Trong số 10 vấn đề về an toàn này, có tổng số 39 mục tiêu và hàng trăm biện pháp điều hành an toàn thông tin tốt nhất được khuyến nghị cho các tổ chức để thỏa mãn các mục tiêu kiểm soát và bảo vệ quyền sở hữu thông tin, chống lại các nguy cơ xâm phạm đến tính bảo mật, tính toàn vẹn và sẵn sàng của thông tin.

**ISO/IEC 27001:2005 (Các yêu cầu – Hệ thống quản lý an toàn thông tin)**

Tiêu chuẩn quốc tế ISO/IEC 27001:2005 xuất phát từ nội dung của tiêu chuẩn BSI (BS7799 phần 2:2002). Nó chỉ ra các yêu cầu để thiết lập, thực thi, vận hành, giám sát, rà soát, duy trì và cải thiện Hệ thống quản lý an toàn thông tin (ISMS) trong một tổ chức. Nó được thiết kế để đảm bảo cho việc chọn lựa và điều hành phù hợp và đầy đủ nhằm bảo vệ tài sản thông tin của tổ chức. Tiêu chuẩn này thường được áp dụng đối với tất cả các tổ chức, bao gồm các doanh nghiệp, cơ quan nhà nước. Tiêu chuẩn này giới thiệu một mô hình tuần hoàn là “Lập kế hoạch – Thực hiện –Kiểm tra – Thi hành” (“Plan-Do-Check-Act” - PDCA) có mục đích thiết lập, thực thi, giám sát và cải thiện hiệu quả Hệ thống quản lý an toàn thông tin. Chu trình PDCA có 4 pha:

• Pha Lập kế hoạch (Plan phase): Thiết lập hệ thống ISMS;

• Pha thực hiện (“Do” phase): Thực thi và vận hành hệ thống;

• Pha kiểm tra (“Check” phase): Giám sát và rà soát hệ thống ISMS;

• Pha thi hành (“Act” phase): Duy trì và cải thiện hệ thống ISMS;

Thông thường, ISO/IEC 27001:2005 được thực hiện cùng với ISO/IEC 27002:2005. ISO/IEC 27001 định nghĩa các yêu cầu cho hệ thống ISMS và sử dụng ISO/IEC 27002 để đưa ra các hoạt động kiểm soát an toàn thông tin phù hợp nhất bên trong Hệ thống ISMS. ISO/IEC 27002 là một bộ quy tắc thực thi cung cấp các hoạt động kiểm soát mà tổ chức có thể ban hành để khuyến cáo các nguy cơ về an toàn thông tin. Các hoạt động kiểm soát này là không bắt buộc. Vì vậy mà không có việc chứng nhận cho ISO/IEC 27002, nhưng một tổ chức có thể được chứng nhận phù hợp với tiêu chuẩn ISO/IEC 27001 nếu quy trình quản lý tuân thủ tiêu chuẩn hệ thống ISMS. Danh sách các cơ quan chứng nhận chính thức có thể chứng nhận một tổ chức tuân thủ tiêu chuẩn ISMS trên wesite về dịch vụ chỉ định của UK.

**ISO/IEC 15408 (Tiêu chuẩn đánh giá cho an toàn công nghệ thông tin)**

Tiêu chuẩn quốc tế ISO/IEC 15408 được coi là Tiêu chuẩn chung “Common Criteria - CC”. Tiêu chuẩn này bao gồm 03 phần: ISO/IEC 15408-1:2005 (giới thiệu và mô hình chung), ISO/IEC 15408-2:2005 (các yêu cầu tính năng an toàn) và ISO/IEC 15408-3:2005 (các yêu cầu bảo đảm an toàn). Tiêu chuẩn này giúp tính toán, phê chuẩn và xác nhận việc bảo đảm an toàn cho một sản phẩm công nghệ phù hợp với một số các thông số như là các yêu cầu tính năng an toàn được chỉ ra trong tiêu chuẩn. Phần cứng và phần mềm được đánh giá phù hợp với các yêu cầu tiêu chuẩn chung (CC) tại các phòng thí nghiệm đo kiểm được chỉ định để chứng nhận Mức độ bảo đảm ước lượng EAL cho các sản phẩm và hệ thống thông tin. Có 7 loại EAL: EAL1 – đo tính năng, EAL2 – đo cấu trúc, EAL3- Đo kiểm theo phương pháp, EAL4 - thiết kế, đo và đánh giá theo phương pháp, EAL5- thiết kế và thử nghiệm bán chính thức, EAL6- thiết kế, thử nghiệm và xác nhận, EAL7- thiết kế, đo, xác nhận chính thức.

Danh sách các cơ quan chỉ định và các sản phẩm đã được đánh giá trên Website tiêu chuẩn chung. Danh sách các sản phẩm được đánh giá tại Mỹ có trên website của Hệ thống đánh giá và xác nhận cho an toàn công nghệ thông tin (CCEVS).

**Tiêu chuẩn ISO/IEC 13335 (Quản lý an toàn công nghệ thông tin)**

Tiêu chuẩn ISO/IEC 13335 ban đầu là một Báo cáo kỹ thuật (TR) trước khi trở thành một tiêu chuẩn ISO/IEC đầy đủ. Tiêu chuẩn này bao gồm tập hợp các hướng dẫn về các biện pháp kỹ thuật kiểm soát an toàn:

a) ISO/IEC 13335-1:2004: Dẫn chứng những khái niệm và mô hình cho quản lý an toàn công nghệ thông tin và truyền thông;

b) ISO/IEC TR 13335-3:1998 dẫn chứng những kỹ thuật cho an toàn thông tin.

c) ISO/IEC TR 13335-4:2000 bao gồm các lựa chọn cho hoạt động bảo vệ (kiểm soát kỹ thuật an toàn), phần này đang được xem xét lại và có thể được thay thế bởi ISO/IEC 27005.

d) ISO/IEC TR 13335-5:2001 gồm việc hướng dẫn quản lý về an toàn mạng. Phần này đang được xem xét lại và có thể được hợp nhất vào tiêu chuẩn ISO/IEC 18028-1 và ISO/IEC 27005.

## Tổ chức quản lý an toàn thông tin

Trong những diễn biến phức tạp về tội phạm mạng, cũng như những phát triển mạnh mẽ của ngành an toàn thông tin, đòi hỏi cần có một tổ chức chịu trách nhiệm quản lý an toàn thông tin quốc gia, đó cũng là lý do Cục An toàn thông tin - tổ chức trực thuộc Bộ Thông tin và Truyền thông được thành lập

**Vị trí và chức năng**

Cục An toàn thông tin là tổ chức trực thuộc Bộ Thông tin và Truyền thông thực hiện chức năng tham mưu, giúp Bộ trưởng Bộ Thông tin và Truyền thông quản lý nhà nước và tổ chức thực thi pháp luật về an toàn thông tin.

Cục An toàn thông tin có tư cách pháp nhân, có con dấu và tài khoản riêng để giao dịch theo qui định của pháp luật, có trụ sở chính đặt tại thành phố Hà Nội.

**Nhiệm vụ và quyền hạn**

Cục An toàn thông tin có nhiệm vụ và quyền hạn sau:

1. Chủ trì nghiên cứu, đề xuất và thực hiện việc xây dựng, sửa đổi, bổ sung trình Bộ trưởng dự thảo các văn bản quy phạm pháp luật thuộc thẩm quyền ban hành của Quốc hội, Ủy ban Thường vụ Quốc hội, Chính phủ, Thủ tướng Chính phủ về an toàn thông tin.

2. Chủ trì, phối hợp xây dựng, trình Bộ trưởng hoặc để Bộ trưởng trình cấp có thẩm quyền phê duyệt chiến lược, quy hoạch, kế hoạch phát triển dài hạn, năm năm, hàng năm, chương trình mục tiêu quốc gia, chương trình hành động, các chương trình, đề án, dự án về an toàn thông tin, giải pháp bảo đảm an toàn thông tin cho hệ thống thông tin quan trọng và tổ chức thực hiện sau khi được phê duyệt theo phân công của Bộ trưởng.

3. Trình Bộ trưởng ban hành theo thẩm quyền văn bản quy phạm pháp luật về an toàn thông tin.

4. Hướng dẫn, tổ chức thực hiện và phối hợp thanh tra, kiểm tra việc thực hiện các văn bản quy phạm pháp luật, các chính sách, chiến lược, quy hoạch, kế hoạch phát triển về an toàn thông tin; các chương trình, đề án, dự án, giải pháp bảo đảm an toàn thông tin cho hệ thống thông tin quan trọng; tuyên truyền phổ biến, giáo dục pháp luật về an toàn thông tin.

5. Trình Bộ trưởng hoặc cấp, gia hạn, sửa đổi, bổ sung, đình chỉ, thu hồi theo thẩm quyền giấy phép, giấy chứng nhận đủ điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin; giấy phép, giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số, giấy công nhận chữ ký số và chứng thư số nước ngoài theo quy định của pháp luật.

6. Trình Bộ trưởng hoặc cấp theo thẩm quyền giấy phép nhập khẩu, giấy chứng nhận lưu hành, giấy chứng nhận hợp chuẩn, hợp quy về an toàn thông tin.

7. Chủ trì, phối hợp và điều phối các tổ chức, cá nhân liên quan ngăn chặn, chống thư rác; cấp mã số quản lý cho nhà cung cấp dịch vụ quảng cáo bằng thư điện tử, nhà cung cấp dịch vụ quảng cáo bằng tin nhắn, nhà cung cấp dịch vụ nội dung qua tin nhắn, nhà cung cấp dịch vụ tin nhắn qua Internet; cấp tên định danh cho nhà cung cấp dịch vụ quảng cáo bằng tin nhắn, nhà cung cấp dịch vụ nội dung qua tin nhắn.

8. Tổ chức đánh giá, kiểm định về an toàn thông tin theo quy định của pháp luật.

9. Giám sát, đôn đốc công tác bảo vệ an toàn hệ thống thông tin theo cấp độ; thẩm định về an toàn thông tin đối với hồ sơ thiết kế hệ thống thông tin; xác nhận cấp độ an toàn thông tin của hệ thống thông tin.

10. Chủ trì, phối hợp hướng dẫn công tác tổ chức bảo đảm an toàn thông tin tại các bộ, ngành, địa phương, doanh nghiệp và các cơ quan, tổ chức khác trên phạm vi toàn quốc; hướng dẫn chuyển giao giải pháp kỹ thuật, công nghệ, quy trình bảo đảm an toàn thông tin.

11. Tổ chức thống kê, thu thập, tổng hợp thông tin, số liệu, khảo sát, đánh giá hiện trạng công tác bảo đảm an toàn thông tin theo định kỳ và đột xuất; dự báo về tình hình an toàn thông tin và cảnh báo các vấn đề về an toàn thông tin.

12. Tổ chức tuyên truyền nâng cao nhận thức về an toàn thông tin; tổ chức các hoạt động thúc đẩy công tác bảo đảm an toàn thông tin thông qua việc tổ chức sự kiện, hội thảo, trao đổi cung cấp thông tin, tài liệu trên các phương tiện truyền thông và các hoạt động hỗ trợ khác.

13. Hợp tác quốc tế về an toàn thông tin theo phân cấp của Bộ trưởng.

14. Phối hợp với các cơ quan, đơn vị liên quan trong công tác đào tạo, cấp chứng chỉ, bồi dưỡng, phát triển nguồn nhân lực về an toàn thông tin; nghiên cứu, xây dựng tiêu chuẩn, quy chuẩn kỹ thuật; ứng dụng khoa học và công nghệ về an toàn thông tin.

15. Phối hợp với các cơ quan, đơn vị liên quan của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ và các cơ quan có liên quan khác trong công tác bảo đảm quốc phòng, an ninh và trật tự, an toàn xã hội; công tác bảo mật thông tin theo quy định của pháp luật.

16. Hướng dẫn, theo dõi và kiểm tra hoạt động của các hội, hiệp hội hoạt động về an toàn thông tin theo quy định của pháp luật.

17. Thu, quản lý và sử dụng phí, lệ phí về an toàn thông tin theo quy định của pháp luật.

18. Tổ chức thực hiện kế hoạch cải cách hành chính của Cục theo chương trình cải cách hành chính của Bộ; hiện đại hóa công sở và ứng dụng công nghệ thông tin phục vụ hoạt động của Cục; báo cáo thực hiện cải cách hành chính hàng năm trong phạm vi quản lý của Cục.

19. Giải quyết khiếu nại, tố cáo; chống tham nhũng, tiêu cực; ngăn chặn, phòng ngừa các hành vi vi phạm pháp luật về an toàn thông tin theo quy định của pháp luật.

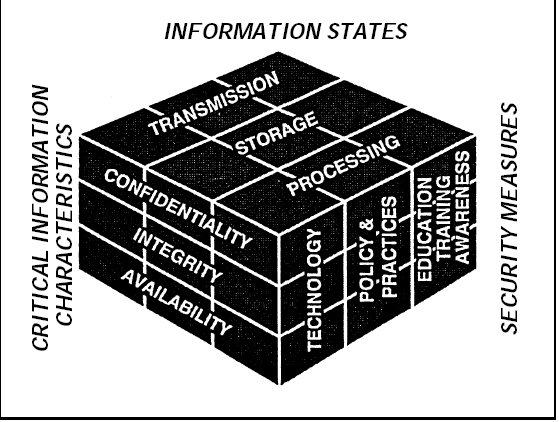
20. Quản lý tổ chức bộ máy, biên chế; thực hiện chính sách, chế độ đối với các cán bộ, công chức, viên chức và lao động thuộc phạm vi quản lý của Cục.

21. Quản lý tài chính, tài sản và các nguồn lực khác được giao; tổ chức thực hiện theo quy định của pháp luật.

22. Thực hiện các nhiệm vụ, quyền hạn khác do Bộ trưởng giao.

## Mô hình, chính sách đảm bảo an toàn thông tin

Bộ ba các đặc tính then chốt của thông tin đề cập đến ở trên bao trùm toàn bộ các mặt của việc đảm bảo an toàn thông tin. Một ma trận được tạo nên bởi 3 yếu tố là 3 trạng thái của thông tin (truyền dẫn, lưu giữ, xử lí) được minh họa ở trục hoành; cùng với 3 đăc tính then chốt của thông tin (độ tin cậy, tính toàn vẹn, tính sẵn sàng) được minh họa trên trục tung có thể được sử dụng làm nền tảng cho mô hình thể hiện các biện pháp an toàn thông tin được trình bày trong phạm vi tài liệu này

****

*Hình 1: Cơ sở cho một mô hình tổng quát*

Các biện pháp an toàn hệ thông thông tin được phân loại thành 3 lớp như sau, tạo thành chiều thứ 3 của không gian ma trận:

* **Các biện pháp công nghệ:** bao hàm tất cả các biện pháp thiết bị phần cứng, các phần mềm, phần sụn (firmware) cũng như các kỹ thuật công nghệ liên quan được áp dụng nhằm đảm các yêu cầu an toàn của thông tin trong các trạng thái của nó như đã kể trên.
* **Các biện pháp về tổ chức:** đưa ra các chính sách, quy định, phương thức thực thi. Thực tế cho thấy, an toàn thông tin không chỉ đơn thuần là vấn đề thuộc phạm trù công nghệ, kỹ thuật. Hệ thống chính sách và kiến trúc tổ chức đóng một vai trò hữu hiệu trong việc đảm bảo an toàn thông tin.
* **Các biện pháp về đào tạo, tập huấn, nâng cao nhận thức:** Các biện pháp công nghệ hay các biện pháp về tổ chức thích hợp phải dựa trên các biện pháp đào tạo, tập huấn và tăng cường nhận thức để có thể triển khai đảm bảo an toàn thông tin từ nhiều hướng khác nhau. Các nhà nghiên cứu và các kỹ sư cũng cần phải hiểu rõ các nguyên lý an toàn hệ thống thông tin, thì mới mong các sản phẩm và hệ thống do họ làm ra đáp ứng được các nhu cầu về an toàn thông tin của cuộc sống hiện tại đặt ra.

Mô hình ma trận không gian 3 chiều kể trên có thể áp dụng làm cơ sở cho đánh giá an toàn thông tin một cách khái quát nhất. Ví dụ, người đánh giá an toàn thông tin cho một sản phẩm là một hệ thống thông tin sẽ phải xác định các trạng thái thông tin trong hệ thống cần được đánh giá. Mô hình tổng quát này sẽ cho phép xác định các trạng thái thông tin không bị lên thuộc vào bất kỳ công nghệ cụ thể nào đang được áp dụng.

## Các biện pháp đảm bảo an toàn thông tin

**Mã hóa thông tin**

Mật mã hay mã hóa dữ liệu (cryptography), là một công cụ cơ bản thiết yếu của bảo mật thông tin. Mật mã đáp ứng được các nhu cầu về tính bảo mật (confidentiality), tính chứng thực (authentication) và tính không từ chối (non-repudiation) của một hệ truyền tin.

Mật mã bao gồm : Lập mã và phá mã. Lập mã bao gồm hai quá trình: mã hóa và giải mã. Để bảo vệ thông tin trên đường truyền người ta thường biến đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền đi trên mạng, quá trình này được gọi là mã hoá thông tin (encryption), ở trạm nhận phải thực hiện quá trình ngược lại, tức là biến đổi thông tin từ dạng không nhận thức được (dữ liệu đã được mã hoá) về dạng nhận thức được (dạng gốc), quá trình này được gọi là giải mã. Đây là một lớp bảo vệ thông tin rất quan trọng và được sử dụng rộng rãi trong môi trường mạng. Để bảo vệ thông tin bằng mật mã người ta thường tiếp cận theo hai hướng:

- Theo đường truyền (Link\_Oriented\_Security).

- Từ nút đến nút (End\_to\_End). Theo cách thứ nhất thông tin được mã hoá để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và đích của thông tin đó. Ở đây ta lưu ý rằng thông tin chỉ được bảo vệ trên đường truyền, tức là ở mỗi nút đều có quá trình giải mã sau đó mã hoá để truyền đi tiếp, do đó các nút cần phải được bảo vệ tốt. Ngược lại theo cách thứ hai thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽ được mã hoá ngay sau khi mới tạo ra và chỉ được giải mã khi về đến đích. Cách này mắc phải nhược điểm là chỉ có dữ liệu của người d­ùng thì mới có thể mã hóa được còn dữ liệu điều khiển thì giữ nguyên để có thể xử lý tại các nút

**An toàn vật lý**

Đây lúc mức bảo vệ thấp nhất nhằm ngăn cản các truy nhập vật lý vào hệ thống công nghệ thông tin của tổ chức. Các biện pháp an ninh vật lý thường được sử dụng để theo dõi, giám sát và ngăn cấm tuyệt đối người không phận sự vào phòng máy chủ, hay không cho phép sử dụng các cổng kết nối thiết bị ngoại vi tới hệ thống khi họ đã tiếp cận.

**Quản trị và Giám sát hệ thống**

Trong thời đại phát triển của công nghệ thông tin, mạng máy tính quyết định toàn bộ hoạt động của một cơ quan, hay một công ty xí nghiệp. Vì vậy việc bảo đảm cho hệ thống mạng máy tính hoạt động một cách an toàn, không xảy ra sự cố là một công việc cấp thiết hàng đầu. Công tác quản trị mạng và giám sát hệ thống máy tính phải được thực hiện một cách khoa học đảm bảo các yêu cầu sau :

- Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc.

- Có hệ thống dự phòng khi có sự cố về phần cứng hoặc phần mềm xảy ra.

- Backup dữ liệu quan trọng theo định kỳ.

- Bảo dưỡng mạng theo định kỳ.

- Bảo mật dữ liệu, phân quyền truy cập, tổ chức nhóm làm việc trên mạng

- Đảm bảo giám sát 24/7 các hoạt động truy xuất hệ thống.

# Lỗ hổng bảo mật và các điểm yếu hệ thống

## Tổng quan về Lỗ hổng bảo mật

**Khái niệm**

Các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, cho phép kẻ tấn công có thể thêm quyền đối với người sử dụng hoặc thực hiện các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể nằm ngay các dịch vụ cung cấp như sendmail, web, ftp ... Ngoài ra các lỗ hổng còn tồn tại ngay chính tại hệ điều hành như trong WindowsXP, Windows 7, \*NIX; hoặc trong các ứng dụng mà người sử dụng thường xuyên sử dụng như Word processing, Các hệ databases...

**Đánh giá lỗ hổng bảo mật**

Là hình thức kiểm tra hệ thống CNTT để xem xét hệ thống đó có thể bị tấn công hay không, bằng cách thực hiện công việc dò quét lên đối tượng cần kiểm tra. Đây là quá trình xem xét lại các dịch vụ và hệ thống để tìm ra các vấn đề an ninh tiềm tàng hoặc dò tìm các dấu vết khi hệ thống bị tổn thương. Từ đó liệt kê các danh sách lỗi gặp phải và đưa ra giải pháp khuyến nghị để tăng cường khả năng bảo mật cho hệ thống.

**Phương pháp gia cố**

Việc gia cố giúp giảm thiểu nguy cơ đối mặt với các lỗ hổng đã được biết đến, gây mất an toàn thông tin cho hệ thống. Để tiến hành gia cố một hệ thống chúng ta có thể thực hiện các công việc như:

* Cập nhật thường xuyên các bản vá bảo mật cho hệ thống
* Giới hạn quyền truy cập tới hệ thống
* Phân quyền người dùng trong hệ thống
* Thực hiện việc đánh giá hệ thống thường xuyên theo định kỳ
* Sử dụng các phần mềm bảo mật có uy tín
* Theo dõi 24/7 các hoạt động bất thường diễn ra trên hệ thống
* …

## Phương pháp đánh giá lỗ hổng bảo mật

**Đánh giá hộp trắng**

Đánh giá hộp trắng là kỹ thuật đánh giá an toàn thông tin trong đó người đánh giá được biết toàn bộ các thông tin liên quan đến mục tiêu đánh giá, bao gồm:

* Bản đồ mạng: Sơ đồ bố trí toàn bộ hệ thống mạng, vị trí thiết đặt Switch, Router, Firewall, IDS/IPS, …. và địa chỉ IP cụ thể của từng trang thiết bị.
* Tài khoản và mật khẩu đăng nhập vào hệ thống, thiết bị mạng, Website, …
* Các nguy cơ thường xảy đến đối với hệ thống (nếu có).
* Mã nguồn ứng dụng và một số vấn đề khác liên quan.

Kỹ thuật đánh giá hộp trắng cho phép thực hiện đánh giá theo một khía cạnh toàn diện, nhìn nhận được tất cả vấn đề liên quan đến tổng thể hệ thống. Tuy nhiên kỹ thuật này đòi hỏi độ phức tạp cao đặc biệt khi thực hiện đánh giá mã nguồn. Với khối lượng lớn các mã dòng lệnh và mối liên hệ phức tạp trong ứng dụng thì rõ ràng việc tiếp cận bằng quan sát mã nguồn không phải đơn giản. Hơn nữa, không phải ứng dụng nào cũng dễ dàng có được mã nguồn phát triển cho người kiểm tra có thể quan sát.

Trong thực tế, kỹ thuật đánh giá hộp trắng thường ít được sử dụng bởi lẽ không phải kẻ tấn công nào cũng có thể tiếp cận, hiểu sâu sắc về hệ thống như một người quản trị hệ thống. Kỹ thuật này chỉ sử dụng khi thời gian và kinh phí hạn chế.

**Đánh giá hộp đen**

Đánh giá hộp đen là kỹ thuật đánh giá an toàn thông tin trong đó người đánh giá hoàn toàn không nắm được bất kỳ thông tin nào về hệ thống đánh giá, mà chỉ có một số thông tin cơ bản như: tên công ty, địa chỉ thực hiện đánh giá, mục tiêu đánh giá, ….

Để thực hiện đánh giá, người đánh giá cần đóng vai trò như 1 kẻ tấn công, thực hiện các bước thu thập thông tin về mục tiêu, phân tích thông tin và tiến hành các thử nghiệm tấn công để tìm ra các điểm yếu tồn tại trong hệ thống.

Kỹ thuật đánh giá hộp đen được cho là kỹ thuật đánh giá chính xác và thực tế nhất. Kỹ thuật này hiện thường được các tổ chức áp dụng để đánh giá cho các hệ thống mạng, Website. Thời gian thực hiện một lần đánh giá khoảng 2 đến 3 tháng cho toàn bộ hệ thống.

**Đánh giá hộp xám**

Đánh giá hộp xám là kỹ thuật đánh giá an toàn thông tin trong đó người đánh giá có được một phần thông tin về mục tiêu đánh giá, như:

* Bản đồ mạng: Sơ đồ bố trí toàn bộ hệ thống mạng, vị trí thiết đặt Switch, Router, Firewall, IDS/IPS, ….
* Tài khoản và mật khẩu đăng nhập vào hệ thống, thiết bị mạng, Website, … Các tài khoản này là tài khoản người dùng bình thường, chứ không phải tài khoản quản trị.

Kỹ thuật đánh giá hộp xám tương tự như kỹ thuật đánh giá hộp đen. Tuy nhiên thay vì đóng vai trò như một người sử dụng cuối, người đánh giá có thể đóng vai trò như một người dùng bình thường trong hệ thống và thực hiện các thử nghiệm tấn công về leo thang đặc quyền vào hệ thống.

Trong thực tế, kỹ thuật này thường ít được sử dụng bởi vì đứng trên vai trò là người quản trị hệ thống, muốn được đánh giá một cách khách quan theo kỹ thuật đánh giá hộp đen. Ngoài ra các thông tin được cung cấp cũng không giúp ích nhiều cho người đánh giá. Nếu một hệ thống có điểm yếu, có thể thực hiện tấn công thì người đánh giá cũng có thể sử dụng các phương pháp thu thập thông tin để thu được các thông tin tương tự các thông tin được cung cấp từ trước.

## Các bước thực hiện đánh giá lỗ hổng bảo mật

Để thực hiện đánh giá hoặc kiểm định an toàn hệ thống thông tin, người đánh giá (kiểm định) cần phải có một quy trình thực hiện nhất định. Theo NIST, quy trình này được chia thành 3 giai đoạn như sau:

* Giai đoạn 1: Lập kế hoạch
* Giai đoạn 2: Thực hiện
* Giai đoạn 3: Sau thực hiện

**Lập kế hoạch**

Để cho một cuộc đánh giá hoặc kiểm định thành công, thì giai đoạn lập kế hoạch là vô cùng quan trọng. Trong bước này, các bên liên quan cần thỏa thuận về mục tiêu đánh giá (kiểm định) và thống nhất thời gian, địa điểm, nhân lực, yêu cầu, …... Đồng thời cũng cần xác định những quy định chung làm cơ sở pháp lý cho các hoạt động diễn ra trong suốt quá trình thực hiện.

Các công việc chính trong quá trình lập kế hoạch và chuẩn bị bao gồm:

* Xác định mục tiêu, phạm vi thực hiện đánh giá (kiểm định)
* Xác định thời gian, địa điểm, nhân lực thực hiện
* Thống nhất phương pháp thực hiện, các công cụ hỗ trợ trong quá trình thực hiện
* Kinh phí thực hiện
* Các thủ tục, giấy tờ liên quan

**Thực hiện**

Sau khi có được các thỏa thuận về mục tiêu, phương pháp, đối tượng và thời gian thực hiện, bước tiếp theo trong quy trình đánh giá hoặc kiểm định an toàn hệ thống thông tin là tiến hành thực hiện. Đây là giai đoạn chiếm tới 80% thời gian trong toàn bộ quy trình.

Mục tiêu chính của giai đoạn này là thực hiện các phương pháp kiểm tra để xác định lỗ hổng và các điểm yếu trong hệ thống mạng. Tùy từng phương pháp thực hiện mà có các quy trình thực hiện khác nhau. Hiện nay có 3 phương pháp phổ biến được sử dụng rộng rãi là ISSAF, OSSTMM và OWASP. Thông thường, các nhiệm vụ cần thực hiện là:

* Thu thập thông tin
* Dò quét, điểm danh và lập bản đồ mạng
* Xác định các dịch vụ đang hoạt động
* Xác định lỗ hổng
* Khai thác mục tiêu
* Leo thang đặc quyền
* Duy trì truy cập

Với các kỹ thuật đánh giá hộp trắng hoặc đánh giá hộp xám, người đánh giá đã có một phần hoặc toàn bộ các thông tin liên quan đến mục tiêu đánh giá thì sẽ bỏ quả một số bước như trên mà chủ yếu tập trung vào xác định lỗ hổng và thực hiện xâm nhập. Tuy nhiên với kỹ thuật đánh giá hộp đen, người đánh giá chưa có bất kỳ thông tin nào về mục tiêu thì sẽ cần thực hiện toàn bộ các nhiệm vụ để có thể thực hiện đánh giá.

Tương tự như đánh an toàn hệ thống thông tin, đối với kiểm định an toàn hệ thống thông tin, sau khi xác định được đối tượng và phạm vi kiểm định, người kiểm định cũng cần thực hiện các công việc để xác định khả năng đáp ứng về an toàn thông tin của hệ thống. Các công việc này thường được thực hiện thông qua việc kiểm tra, hoặc phỏng vấn các đối tượng liên quan như bộ phận quản trị mạng, trưởng phòng, nhân viên trong phòng, …. Các thông tin thu được từ quá trình kiểm định sẽ là căn cứ để khẳng định hệ thống đã đáp ứng được các yêu cầu về an toàn thông tin hay chưa, và là cơ sở cho việc cấp chứng nhận kiểm định.

**Sau thực hiện**

Giai đoạn cuối cùng trong quy trình đánh giá hoặc kiểm định an toàn hệ thống thông tin là tập trung vào phân tích các lỗ hổng để xác định mức độ nghiêm trọng của chúng, đồng thời đưa ra các khuyến nghị cho từng lỗ hổng. Tất cả quy trình thực hiện cũng như danh sách các lỗ hổng, các khuyến nghị cần được thể hiện trong một báo cáo cuối cùng. Ngoài ra, người đánh giá (kiểm định) cũng cần làm sạch các vấn đề liên quan trong quá trình thực hiện, như gỡ bỏ các tài khoản sử dụng khi thực hiện đánh giá, đóng các cổng đã mở trên thiết bị phục vụ quá trình quét hệ thống, ….

## Đánh giá an toàn cho hệ thống

### Hệ điều hành Windows

Microsoft Windows là một hệ điều hành phổ biến, và thường được sử dụng trong các hệ thống mạng. Windows có 2 phiên bản: 1 phiên bản Windows Server (Windows Server 2008, Windows Server 2012, …) dành cho các máy chủ và 1 phiên bản Windows (Windows 7, Windows 8, …) dành cho các máy trạm. Chính vì tính phổ biến và được ưa dùng nên hệ điều hành Windows luôn được các hacker chú trọng khai thác. Mặc dù Microsoft thường xuyên đưa ra các bản vá lỗi cho các phiên bản hệ điều hành Windows nhưng kẻ tấn công vẫn có thể lợi dụng để khai thác các kẽ hở, thực hiện tấn công xâm nhập chiếm quyền điều khiển hệ thống.

Để đánh giá an toàn cho hệ điều hành Windows, người đánh giá cần thực hiện các kiểm tra tấn công vào hệ thống. Các kiểm tra này có thể là kiểm tra tấn công mật khẩu hoặc tấn công lợi dụng điểm yếu trong các dịch vụ trên hệ điều hành.

**Kiểm tra tấn công mật khẩu**

Mặc định sau khi cài đặt xong, Windows sẽ có 2 tài khoản mặc định là Administrator và Guest. Nếu người quản trị đăng ký thêm tài khoản thì các tài khoản sẽ có giá trị và quyền hạn sử dụng theo nhóm được gán. Như vậy để thực hiện tấn công mật khẩu, phương pháp đầu tiên người đánh giá cần thực hiện là đoán mật khẩu theo các cụm từ khóa phổ biến.

*Ví dụ:*

|  |  |
| --- | --- |
| **Tên tài khoản** | **Mật khẩu** |
| admin  administrator  user1  test  guest1  abc  *(tên người dùng)* | 123  123456  1234567  abc  abcdef  password  matkhau  khongbiet  admin  admin@123  pasw0rd  *(các thông tin liên quan tới cá nhân)* |

Tiếp theo, người đánh giá cần thử tấn công vào hệ thống để lấy các tài khoản khác đặc biệt là tài khoản quản trị và file SAM của hệ thống. Khi đã có các thông tin về file SAM, có thể sử dụng tiếp các chương trình bẻ mật khẩu như L0ptCrack, OphCrack, RainBow, … để bẻ các mật khẩu của những người sử dụng khác trong hệ thống.

Như chúng ta đã biết hệ điều hành Windows có một cơ chế là SID (Security Identifier) để gán định danh cho người dùng. Mặc định tài khoản Administrator có SID = 500 và tài khoản Guest có SID = 501. Khi người quan trị tạo thêm các tài khoản thì số SID sẽ tính từ 1001 trở lên. Bên cạnh đó, mặc định Windows sẽ có một số tài nguyên chia sẻ là:

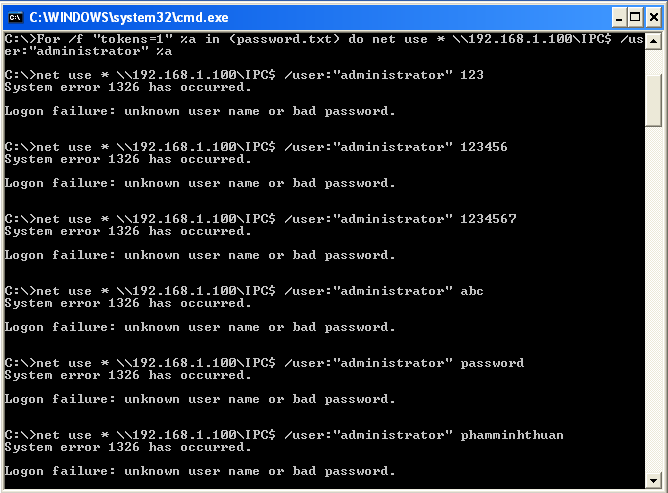
* Ổ\_đĩa$ (ví dụ: C$, D$, …): Là các ổ đĩa được chia sẻ.
* ADMIN$: Là nguồn tài nguyên được sử dụng khi thực hiện quản trị từ xa.
* IPC$: Là tài nguyên chia sẻ để kết nối giữa các chương trình. Tài nguyên này không thể bị xóa.
* NETLOGON: Là tài nguyên chia sẻ được sử dụng trên DC.
* SYSVOL: Là tài nguyên chia sẻ được sử dụng trên DC.
* **PRINT$: Là tài nguyên được sử dụng khi quản trị máy in từ xa**
* **FAX$**: Là một thư viện chia sẻ trên server được sử dụng khi truyền fax.
* NETLOGON VÀ SYSVOL là các tài nguyên chia sẻ không ẩn. Đây là các chia sẻ đặc biệt về quản trị.

Lợi dụng các tài nguyên chia sẻ mặc định này, kẻ tấn công có thể thực hiện xâm nhập vào hệ thống sử dụng phương pháp bẻ mật khẩu khi đã xác định được một tài khoản bất kỳ có trong hệ thống. Dưới đây là một ví dụ về thực hiện tấn công bẻ mật khẩu lợi dụng tài nguyên chia sẻ mặc định lên hệ điều hành Windows:

Giả sử máy bị tấn công địa chỉ IP: 192.168.1.18, máy sử dụng để tấn công cùng nằm trong mạng 192.168.1.0/24. Ta sẽ thực hiện tấn công đề dò tìm mật khẩu của tài khoản Administrator lên tài nguyên chia sẻ mặc định IPC$.

Đầu tiên tạo một file từ điển chứa các mật khẩu thông dụng và đặt tại một thư mục trên ổ đĩa (ví dụ: password.txt)

Sử dụng lệnh for để tạo vòng lặp thử các mật khẩu có trong file password.txt:



*Hình 2: Thử tấn công bẻ mật khẩu trong hệ điều hành Windows*

Nếu có một mật khẩu trùng với mật khẩu được đặt cho tài khoản người sử dụng thì sẽ có thông báo *“The command complete successfully”.* Như vậy chỉ cần dựa vào thông báo ở trên, chúng ta có thể biết được mật khẩu của tài khoản Administrator.

**Kiểm tra lỗ hổng dịch vụ**

Công việc tiếp theo cần thực hiện là kiểm tra các lỗ hổng thông qua các dịch vụ chạy trên hệ điều hành. Phần lớn các dịch vụ chạy thường kèm theo một số lỗ hổng trong đó mà kẻ tấn công có thể lợi dụng để tấn công vào hệ thống. Dưới đây là một số lỗ hổng phổ biến trên các dịch vụ mà người đánh giá cần chú ý khi thực hiện đánh giá an toàn cho hệ điều hành này:

* + - NetBIOS

NetBIOS là một dịch vụ dùng để chia sẻ file trên windows. Tấn công vào NetBIOS kẻ tấn công có thể có được danh sách các tài nguyên được chia sẻ, tài khoản, và đôi khi là truy cập với Admin

Cổng quan trọng nhất của dịch vụ Netbios là 139, tuy nhiên dịch vụ chạy trên cổng 135-139 và 445 cũng thường là Netbios. Nếu NetBIOS được cho phép qua TCP/IP thì chúng ta có thể tấn công NetBIOS thông qua internet

* + - SMB

SMB (Server Messenger Block) là giao thức chia sẻ tập tin. Khi một hệ thống windows muốn truy cập tài nguyên chia sẻ thì giữa các máy sẽ trao đổi với nhau một đoạn mã đã được băm, nếu bắt được các gói tin đó, kẻ tấn công có thể có được mật khẩu khi 2 bên trao đổi thông tin.

* + - Registry

Kẻ tấn công có thể ẩn backdoor và chỉnh sửa trong registry để hệ thống khởi độc mã độc. Backdoor giống như netcat hay keylogger có thể được kích hoạt khi khởi động hệ thống.

*HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*

Như vậy nếu kẻ tấn công có thể sửa đổi register, thì khi hệ thống khởi động, kẻ tấn công có thể dễ dàng truy cập vào hệ thống.

* + - LPC

Có một lỗ hổng trong hàm của LPC (Local Procedure Call) Port API dẫn đến tấn công leo thang đặc quyền. Razor team đã ra một công cụ để khai thác lỗ hổng này tên là hk. Nó cho phép một người dùng bình thường trên hệ thống có được quyền quản trị.

* + - DLL injection

Đây là một ứng dụng dump password hash trong database SAM của Windows NT. Thông tin thu được nhập vào l0phtcrack hoặc sử dụng với Samba. Cần SeDebugPrivilege để nó hoạt động. Theo mặc định, chỉ có administrator mới có quyền này, vì vậy trong windows NT không ảnh hưởng đến security, nhưng trong trường hợp kẻ xâm nhập chạy nó cùng với một số lỗ hổng khác (ví dụ IIS exploit), kẻ xâm nhập sẽ lấy được mật khẩu (đã băm). Và để crack mật khẩu băm chỉ còn là vấn đề thời gian.

### Hệ điều hành Unix/ Linux

Hệ điều hành Windows là hệ điều hành thương mại, mã nguồn không công bố nên kẻ tấn công khó tiếp cận trực tiếp được về mã nguồn hệ thống. Tuy nhiên đối với hệ điều hành Unix/Linux là hệ điều hành mã nguồn mở, khả năng bị tấn công nhiều hơn hệ điều hành windows. Mặc dù các hệ điều hành mã nguồn mở thường xuyên được cộng đồng kiểm nghiệm, đánh giá và đưa ra các khuyến nghị vá lỗi song không phải chỉ như vậy là đã đầy đủ và hệ thống đã an toàn. Do vậy cần phải thường xuyên thực hiện đánh giá để sớm phát hiện ra các lỗ hổng tồn tại trong HĐH để có các biện pháp giải quyết kịp thời.

Để đánh giá an toàn cho hệ điều hành Unix/Linux, người đánh giá cần thực hiện một số kiểm tra các dịch vụ và thử nghiệm các phương pháp tấn công lên hệ thống

**Kiểm tra lỗ hổng dịch vụ**

Kiểm tra dịch vụ đang hoạt động là công việc rất quan trọng khi đánh giá an toàn, bởi vì trong một số dịch vụ có xuất hiện các điểm yếu mà kẻ tấn công có thể dựa vào đó để khai thác. Sau đây chúng ta sẽ liệt kê một số lỗ hổng trong các dịch vụ chạy trên hệ điều hành Unix/Linux thường có chứa điểm yếu:

* + - RWHO

Rwho là một dịch vụ trong /etc/inetd.conf, hoạt động trong mạng nội bộ, kết hợp tất cả thông tin của những người trong mạng nội bộ, nó hoạt động trên cổng 513 UDP. Nếu kẻ tấn công lợi dụng dịch vụ này để tấn công thì có thể kiểm soát được các hoạt động trong mạng nội bộ của hệ thống.

\* *Ví dụ:*

#rwho -a wally becky smith

becky cygnus:pts0 Jan 17 11:20 :12

smith aquila:ttyp0 Jan 15 09:52 :22

wally lyra:pts7 Jan 17 13:15 1:32

wally lyra:pts8 Jan 17 14:15 1:01

Như vậy, dựa vào các thông tin trên kẻ tấn công có thể thấy chi tiết hoạt động của các người thuộc mạng nội bộ, ở đây wally và becky ở đang ở trạng thái idle trong hơn 1 giờ.

* + - Ruser

Tương tự như rwho, ruser chạy trên cổng 513 UDP. Nếu kẻ tấn công lợi dụng dịch vụ này thì có thể biết được tên máy và tên đăng nhập tới hệ thống.

\* *Ví dụ:*

#rusers -l <target>

[root@localhost root]# rusers -l 192.168.0.60

root 192.168.0.60:tty1 May 11 22:02 :01

root 192.168.0.60:pts/0 May 12 02:00 :01 (192.168.0.100)

root 192.168.0.60:pts/1 May 12 00:35 :16 (192.168.0.1)

root 192.168.0.60:pts/2 May 12 01:39 :15 (192.168.0.70)

gaurav 192.168.0.60:pts/3 May 12 01:41 (192.168.0.1)

Ở ví dụ trên ta sẽ thu được tên máy và tên đăng nhập ngay cả khi máy đó không có ai login

* + - SMTP

SMTP là dịch vụ chạy trên cổng 25 hỗ trợ các VRFY, EXPN, ESMTP, HELP, và EHLO. EXPN và VRFY là hai câu lệnh mà kẻ tấn công có thể sử dụng để điểm danh. Với lệnh EXPN, kẻ tấn công có thể tìm được các bí danh (aliases), từ đó sẽ lập được danh sách các tài khoản quản trị trên máy chủ email. Lệnh VRFY được sử dụng lấy được họ tên của các email trên server, việc này có thể phục vụ cho tấn công social engineering.

*Ví dụ:*

"telnet target 25".

vrfy user

This will produce an output like:

250 kartikeya puri <user@target>

expn all

250-someone somewhere <user@target1>

250-another guy <root@target1>

250-yetanotehr guy <guest@target2>

250-real babe babe@babevilla

Họ tên lấy được có thể được kẻ tấn công sử dụng để đoán các mật khẩu liên quan hoặc sử dụng cho kỹ thuật social engineering

* + - RPCINFO

RPCINFO là dịch vụ dùng để xem các cổng đã đăng ký. Nếu kẻ tấn công khai thác được dịch vụ này thì có thể thăm dò portmap trên mục tiêu.

*Ví dụ:*

#rpcinfo -p target

program vers proto port

100000 4 tcp 111 portmapper

100000 3 tcp 111 portmapper

100000 2 tcp 111 portmapper

100000 4 udp 111 portmapper

100000 3 udp 111 portmapper

100000 2 udp 111 portmapper

100232 10 udp 32772 sadmind

100221 1 tcp 32772

100068 2 udp 32773

100068 3 udp 32773

100068 4 udp 32773

100068 5 udp 32773

300326 4 tcp 32773

100249 1 udp 32778

100249 1 tcp 32779

300598 1 udp 32781

300598 1 tcp 32780

805306368 1 udp 32781

805306368 1 tcp 32780

* + - SNMP

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

SNMP sử dụng 2 chuỗi cộng đồng là public và private, ở một số thiết bị mặc định 2 chuỗi là “public” và “private”. Lợi dụng vào các chuỗi này kẻ tấn công có thể xác định được: hệ điều hành, điểm danh người sử dụng hoặc các tài nguyên chia sẻ, tên hệ thống, dịch vụ, cấu hình của thiết bị (router, firewall,..)

* + - *TFTP*

Giao thức TFTP là một giao thức truyền dữ liệu đơn giản. Nó thường được sử dụng bởi Router, Switch hoặc một số thiết bị khác để kết nối đến TFTP server để nâng cấp firmware. Kẻ tấn công có thể lợi dụng lỗ hổng trong giao thức này để lấy các tập tin mà không cần phải xác thực như: file cấu hình, file log hệ thống, ….

*Ví dụ:*

Kẻ tấn công vào giao diện dòng lệnh TFTP:

#tftp

tftp> \_

sau đó kiểm tra trạng thái:

#tftp

tftp>status

Not connected.

Mode: netascii Verbose: off Tracing: off

Max-timeout: 25 seconds

tftp> \_

=>Trạng thái của chủ nhân chiếc máy hiện tại đang không kết nối.

Thực hiện kết nối đến TFTP server:

tftp>connect <IP mục tiêu>

=>Khi xuất hiện dấu nhắc (>) tức là đã kết nối thành công vào server.

Đoán và thu thập các file:

tftp> get /etc/passwd /tmp/passwd.system

Như vậy, kẻ tấn công đã download file passwd.system thành công

**Kiểm tra tấn công hệ thống**

Để đánh giá an toàn cho hệ điều hành Unix/Linux ngoài việc kiểm tra dịch vụ, dò quét lỗ hổng cần thực hiện các thử nghiệm tấn công. Dưới đây là một số các hình thức kiểm tra tấn công cần thực hiện để đánh giá an toàn cho các hệ điều hành này:

* + - Kiểm tra tấn công mật khẩu

Sử dụng một số biện pháp như: dò đoán, bẻ mật khẩu, sniff hệ thống để đoán mật khẩu. Phương pháp này tương tự như với HĐH Windows.

* + - Kiểm tra lỗi tràn bộ đêm

Trong các lĩnh vực an ninh máy tính và lập trình, một lỗi tràn bộ nhớ đệm hay gọi tắt là lỗi tràn bộ đệm là một lỗi lập trình có thể gây ra một ngoại lệ truy nhập bộ nhớ máy tính và chương trình bị kết thúc, hoặc khi người dùng có ý phá hoại, họ có thể lợi dụng lỗi này để phá vỡ an ninh hệ thống.

Lỗi tràn bộ đệm là một điều kiện bất thường khi một tiến trình lưu dữ liệu vượt ra ngoài biên của một bộ nhớ đệm có chiều dài cố định. Kết quả là dữ liệu đó sẽ đè lên các vị trí bộ nhớ liền kề. Dữ liệu bị ghi đè có thể bao gồm các bộ nhớ đệm khác, các biến và dữ liệu điều khiển luồng chạy của chương trình (program flow control).

Các lỗi tràn bộ đệm có thể làm cho một tiến trình đổ vỡ hoặc cho ra các kết quả sai. Các lỗi này có thể được kích hoạt bởi các dữ liệu vào được thiết kế đặc biệt để thực thi các đoạn mã phá hoại hoặc để làm cho chương trình hoạt động một cách không như mong đợi. Bằng cách đó, các lỗi tràn bộ đệm gây ra nhiều lỗ hổng bảo mật đối với phần mềm và tạo cơ sở cho nhiều thủ thuật khai thác (exploit). Việc kiểm tra biên (bounds checking) đầy đủ bởi lập trình viên hoặc trình biên dịch có thể ngăn chặn các lỗi tràn bộ đệm.

* + - Kiểm tra lỗi Format string

Trong ngôn ngữ lập trình C/C++ có các hàm và đối số các hàm quy định các kiểu dữ liệu khác nhau, nếu trong khi lập trình không có việc kiểm tra các kiểu dữ liệu nhập vào sẽ làm cho chức năng của các hàm bị sai dẫn đến lỗi phần mềm.

* + - Kiểm tra lỗi Parsing Errors

Lỗi cú pháp chủ yếu là do không xử lý đầu vào tới bộ đệm, hầu hết thời gian chương trình sẽ chấp nhận bộ đệm và sau đó phân tích bộ đệm rồi chuyển nó đến chương trình. Khi người dùng được quyền kiểm soát bộ đệm, đây sẽ là một nguy cơ gây tràn bộ đệm.

* + - Kiểm tra NFS Share

Tận dụng cấu hình không chính xác trong /etc/exports, kẻ tấn công có thể thực hiện gắn kết các file hệ thống từ xa và tải xuống tất cả file relev ant, thay đổi cấu hình và đánh cắp thông tin hệ thống.

*Ví dụ:*

#showmount -e target

#mount -t nfs target:/share /mnt

#find /mnt | grep –i password

* + - Kiểm tra X-Insecurities

Hệ thống X Window System cung cấp chức năng cho phép chia sẻ màn hình đồ họa. Vấn đề chính là ở mô hình bảo mật của X. Khi được cấp quyền truy cập vào máy chủ X. Client X có thể bắt được tổ hợp phím của người sử dụng giao diện điều khiển, đóng cửa sổ tùy ý, chụp lại màn hình để phục vụ mục đích khác. Hình thức đơn giản và phổ biến nhất để kiểm soát truy cập máy chủ X là một cơ chế xác thực. Tuy nhiên cơ chế xác thực này không đủ an toàn.

*Ví dụ:*

[localhost]$ xscan target\_machine

Scanning hostname quake ...

Connecting to quake (target\_machine) on port 6000...

Connected.

Host quake is running X.

Starting keyboard logging of host quake:0.0 to file KEYLOGquake:0.0...

Now any keystrokes typed at the console will be captured to the KEYLOG.quake file.

[localhost]$ tail -f KEYLOG.quake:0.0

su -

[Shift\_L]Iamowned[Shift\_R]!

* + - Kiểm tra lỗ hổng RPC

RPC cho phép người quản trị thực thi câu lệnh trên máy tính nối mạng để thực hiện quản lý quy mô lớn hiệu quả hơn. Khi hoạt động, RPC thường hoạt động với quyền cao nhất. Kẻ tấn công thường lợi dụng các lỗ hổng trên giao thức này để tấn công chiếm quyền điều khiển hệ thống.

*Ví dụ:*

[localhost]# cmsd.sh quake 192.168.1.xxx 2 192.168.1.xxx

Executing exploit...

rtable\_create worked

clnt\_call[rtable\_insert]: RPC: Unable to receive; errno = Connection reset by peer

* + - Kiểm tra tấn công Web

Dịch vụ web chạy trên cổng 80, website có thể chứa lỗ hổng để kẻ tấn công có thể chiếm quyền admin của server, thậm chí là chiếm toàn bộ quyền điều khiển của server.

*Ví dụ:*

• http://host/cgi-bin/lame.cgi?file=../../../../etc/motd

• http://host/cgi-bin/lame.cgi?page=ls%20-al|

• http://host/cgi-bin/lame.cgi?page=../../../../bin/ls|

• http://host/cgi-bin/bad.cgi?doh=../../../../bin/rm%20-rf%20\*|

• http://host/cgi-bin/bad.cgi?doh=rm%20-rf%20\*;

• http://host/cgi-bin/bad.cgi?doh=../../../../bin/chown%20zeno%20/etc/master.passwd|

• http://host/cgi-bin/helloworld?type=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

* + - Kiểm tra tấn công Mail

***Tấn công cục bộ***

Tấn công cục bộ được thực hiện khi không có đặc quyền hoặc không thể truy cập vào hệ thống. Phương pháp này thường sử dụng kỹ thuật social engineering.

***Tấn công liên kết tượng trưng***

SUID /SGID files kill

Find SGUID root files

find / -perm -4000 -exec ls -al {} \;

Find SUID root files

find / -perm -2000 -exec ls -al {} \;

Find sticky bit files

find / -perm -1000 -exec ls -al {} \;

Find SGUID root files

[balwant@localhost balwant]$ find / -perm -4000 -exec ls -al {} \;

-rwsr-xr-x 1 root bin 1303552 May 6 10:39 /usr/openwin/bin/Xsun

-rwsr-xr-x 1 root bin 74716 Aug 5 2003 /usr/openwin/bin/xlock

-rwsr-sr-x 1 root bin 22868 May 28 02:49

r/openwin/bin/kcms\_configure

-rwsr-sr-x 1 root bin 94632 May 28 02:53

r/openwin/bin/kcms\_calibrate

-rwsr-xr-x 1 root bin 295400 Mar 19 2004

r/openwin/bin/xscreensaver

-rwsr-xr-x 1 root bin 23180 Oct 17 2002 /usr/openwin/lib/mkcookie

-r-sr-xr-x 1 root sys 13748 Jun 17 02:13 /usr/bin/i86/newtask

-r-sr-xr-x 2 root bin 11272 Nov 4 2002 /usr/bin/i86/uptime

-r-sr-xr-x 2 root bin 11272 Nov 4 2002 /usr/bin/i86/w

/usr/lib/uucp/remote.unknown

---s--x--x 1 uucp uucp 159528 Nov 4 2002 /usr/lib/uucp/uucico

---s--x--x 1 uucp uucp 33408 Nov 4 2002 /usr/lib/uucp/uusched

/usr/dt/bin/sdtcm\_convert

-r-sr-xr-x 1 root bin 349604 Jan 11 2003 /usr/dt/bin/dtprintinfo

-r-sr-xr-x 1 root bin 154544 Apr 15 18:30 /usr/dt/bin/dtsession

[balwant@localhost balwant]$ find / -perm -2000 -exec ls -al {} \;

-r-xr-sr-x 1 root sys 13540 Nov 4 2002 /usr/platform/i86pc/sbin/eeprom

-rwxr-sr-x 1 root root 1474468 Mar 16 2004 /usr/openwin/bin/Xprt

-rwxr-sr-x 1 root root 312936 Oct 17 2002 /usr/openwin/bin/lbxproxy

-rwsr-sr-x 1 root bin 22868 May 28 02:49 /usr/openwin/bin/kcms\_configure

-rwsr-sr-x 1 root bin 94632 May 28 02:53 /usr/openwin/bin/kcms\_calibrate

-r-x--s--x 1 root mail 66256 Dec 14 2002 /usr/bin/mail

-r-x--s--x 1 root mail 118064 Nov 4 2002 /usr/bin/mailx

-r-xr-sr-x 1 root sys 59700 Nov 4 2002 /usr/bin/netstat

-r-sr-sr-x 1 root sys 22168 Nov 4 2002 /usr/bin/passwd

-r-xr-sr-x 1 root tty 11612 Nov 4 2002 /usr/bin/write

-r-xr-sr-x 1 root smmsp 872332 Sep 25 2003 /usr/lib/sendmail

-r-xr-sr-x 1 root sys 22064 Nov 4 2002 /usr/sbin/i86/prtconf

-r-xr-sr-x 1 root sys 10528 Nov 4 2002 /usr/sbin/i86/swap

-r-xr-sr-x 1 root sys 22056 Nov 4 2002 /usr/sbin/i86/sysdef

-r-xr-sr-x 1 root tty 10036 Mar 26 2003 /usr/sbin/wall

-r-sr-sr-x 1 root sys 23092 Sep 21 2002 /usr/dt/bin/dtaction

-r-sr-sr-x 1 root daemon 288084 Sep 21 2002 /usr/dt/bin/sdtcm\_convert

-r-xr-sr-x 1 root mail 1458996 May 4 19:17 /usr/dt/bin/dtmail

-r-xr-sr-x 1 root mail 445972 Jan 11 2003 /usr/dt/bin/dtmailpr

***Tấn công gọi hàm hệ thống***

Gọi hàm hệ thống là một cơ chế mà các chương trình ứng dụng sử dụng để yêu cầu các dịch vụ có sẵn của hệ điều hành. Hay nói cách khác gọi hệ thống cung cấp một giao diện cho các dịch vụ mà hệ điều hành cung cấp.

Ví dụ về gọi hệ thống: Lệnh fork() trong Unix dùng để tạo ra một tiến trình mới.

Chương trình hệ thống là các chương trình cung cấp một môi trường thuận tiện để phát triển và thực thi chương trình. Ứng dụng là chương trình được viết ra để giúp người sử dụng giải quyết một vấn đề nào đó hoặc thao tác trong công việc. Ví dụ như Web Browser, Microsoft Office Word

Vài ví dụ về các chương trình hệ thống là: Compiler, Linker, Loader, Debugger

# Các kỹ thuật tấn công phổ biến vào hệ thống thông tin

## Các kỹ thuật tấn công mạng điển hình

*Social Engineering:* Tấn công này với hai mục đích chính là đùa cợt và trục lợi . Kỹ thuật này phụ thuộc nhiều vào sơ hở của nhân viên, hacker có thể gọi điện thoại hoặc gửi e-mail giả danh người quản trị hệ thống từ đó lấy mật khẩu của nhân viên và tiến hành tấn công hệ thống. Cách tấn công này rất khó ngăn chặn. Cách duy nhất để ngăn chặn nó là giáo dục khả năng nhận thức của nhân viên về cách đề phòng.

*Impersonation(mạo danh)* là ăn cắp quyền truy cập của người sử dụng có thẩm quyền. Có nhiều cách kẻ tấn công như một hacker có thể mạo danh một người dùng hợp pháp. Ví dụ, hacker có thể nghe lén một phiên telnet sử dụng các công cụ nghe lén như tcpdump hoặc nitsniff. Dĩ nhiên sau khi lấy được password, hacker có thể đăng nhập hệ thống như là người dùng hợp pháp.

*Exploits (khai thác lỗ hổng):* tấn công này liên quan đến việc khai thác lỗi trong phần mềm hoặc hệ điều hành. Do gấp rút hoàn thành để đáp ứng nhu cầu của thị trường, các phần mềm thường chưa được kiểm tra lỗi kỹ ngay cả trong dự án phần mềm lớn như hệ điều hành lỗi này cũng rất phổ biến. Các hacker thường xuyên quét các host trong mạng để tìm các lỗi này và tiến hành thâm nhập.

*Data Attacks (tấn công dữ liệu):* Lập trình Script đã mang lại sự linh động cho sự phát triển của Web và bên cạnh đó cũng mang lại sự nguy hiểm cho các hệ thống do các đoạn mã độc. Những script hiện hành có thể chạy trên cả server (thường xuyên) và client. Bằng cách đó, các script có thể gửi mã độc vào hệ thống như trojan, worm, virus…

*Tấn công vào điểm yếu cơ sở hạ tầng:* Một số điểm yếu lớn nhất của cơ sở hạ tầng mạng được tìm thấy trong các giao thức truyền thông. Đa số hacker nhờ kiến thức về cơ sở hạ tầng sẵng có đã tận dụng những lỗ hổng và sử dụng chúng như là nơi tập trung để tấn công. Có nhiều lỗ hổng của các giao thức truyền thông và đã có bản vá những lỗi này tuy nhiên do sự mất cảnh giác không cập nhật bản vá kịp thời của những người quản trị hệ thống mà các hacker có thể tận dụng những lỗ hổng này để tấn công. Dĩ nhiên hacker sẽ phải liên tục quét hệ thống để tìm những lỗ hổng chưa được vá lỗi.

*Tấn công Từ chối dịch vụ:* Đây là kỹ thuật tấn công rất được ưa chuộng của hacker. Loại tấn công này chủ yếu tập trung lưu lượng để làm ngưng trệ các dịch vụ của hệ thống mạng. Hệ thống được chọn sẽ bị tấn công dồn dập bằng các gói tin với các địa chỉ IP giả mạo. Để thực hiện được điều này hacker phải nắm quyền kiểm soát một số lượng lớn các host trên mạng (thực tế các host này không hề biết mình đã bị nắm quyền kiểm soát bởi hacker) từ đó tập trung yêu cầu đến dịch vụ của hệ thống đích cho đến khi dịch vụ bị ngưng trệ hoàn toàn.

*Active Wiretap:* Trong kiểu tấn công này, dữ liệu sẽ bị chặn lại trong quá trình truyền. Khi bị chặn lại có hai hành động chủ yếu đối với dữ liệu: một là gói tin sẽ bị thay đổi địa chỉ IP nguồn hoặc đích hoặc số thứ tự của gói tin, hai là dữ liệu không bị thay đổi nhưng sẽ bị sao chép để sử dụng cho những mục đích khác.

**Giải pháp phòng chống tấn công**

Tất cả các giải pháp hiện nay điều chỉ giảm thiếu đáng kể các cuộc tấn công vào một tổ chức, không có giải pháp nào là tuyệt đối trong việc phát hiện và ngăn chặn tấn công, tuy nhiên để đảm bảo vấn đề an toàn thông tin cho các tổ chức, doanh nghiệp thì những giải pháp sau cần được triển khai:

* Triển khai hệ thống giám sát an ninh mạng đễ theo dõi, giám sát 24/7 các hoạt động ra vào hệ thống tổ chức, phát hiện sớm các cuộc tấn công đang nhằm vào tổ chức
* Triển khai hệ thống tường lửa và hệ thống ngăn chặn xâm nhập để đánh chặn các cuộc tấn công đã biết trước nhằm vào hệ thống công nghệ thông tin.
* Triển khai các phần mềm diệt virus có uy tín để ngăn chặn tấn công sử dụng mã độc
* Thực hiện rà soát, đánh giá thường xuyên hệ thống công nghệ thông tin để đảm bảo các lỗ hổng, điểm yếu đang tồn tại trên hệ thống được phát hiện sớm và có biện pháp khắc phục
* Triển khai các giải pháp mã hóa để bảo vệ dữ liệu quan trọng khi chúng được lưu trữ trong máy tính cũng như được vận chuyển trên đường truyền.
* Đào tạo nâng cao nhận thức người dùng để tránh các tấn công lửa đảo nhằm người dùng cuối.

## Tấn công lớp 3

*IP Spoofing*

Địa chỉ IP có mục đích để xác định một thiết bị duy nhất trên thế giới. Vì vậy trên mạng một máy chủ có thể cho phép một thiết bị khác trao đổi dữ liệu qua lại mà không cần kiểm tra máy chủ. Tuy nhiên địa chỉ IP có thể thay đổi, việc này cho phép kẻ tấn công có thể gởi một thông tin giả đến một máy khác mà máy đó sẽ tin rằng thông tin nhận được xuất phát từ một máy nào đó bị giả mạo. Kỹ thuật này thường được sử dụng trong việc ẩn danh, vượt tường lửa, hay tấn công từ chối dịch vụ phân tán…

*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, hacker có thể tạo ra nhiều gói tin có giá trị offset trùng lặp nhau gửi đến mục tiêu muốn tấn công. Kết quả là máy tính đích không thể sắp xếp được những gói tin này và dẫn tới bị treo máy vì bị "vắt kiệt" khả năng xử lý.

*Ping of Death*

Bình thường, ping được dùng để kiểm tra xem một host có sống hay không. Một lệnh ping thông thường có hai thông điệp echo request và echo reply. Khi tấn công bằng Ping of Death, một gói tin echo đựoc gửi có kích thước lớn hơn kích thước cho phép là 65,536 bytes. Gói tin sẽ bị chia nhỏ ra thành các segment nhỏ hơn, nhưng khi máy đích ráp lại, host đích nhận thấy rằng là gói tin quá lớn đối với buffer bên nhận. Kết quả là, hệ thống không thể quản lý nổi tình trạng bất thường này và sẽ reboot hoặc bị treo.

*Land Attack.*

Trong kiểu tấn công này, một gói tin TCP SYN sẽ được gửi với cùng địa chỉ nguồn, địa chỉ đích và số cổng. Khi một host nhận được dạng lưu lượng bất thường này, host thường sẽ chậm lại hoặc treo hoàn toàn vì nó cố gắng khởi tạo kết nối với chính nó trong một vòng lặp bất tận. Mặc dù đây là một kiểu tấn công cũ, cả Windows XP với SP2 và Windows server 2003 đều bị ảnh hưởng với kiểu tấn công này. Bạn có thể dùng chương trình Hping để tạo ra các gói tin có cùng địa chỉ nguồn và địa chỉ đích.

## Tấn công lớp 4

*SYN Flooding*

Kiểu tấn công TCP SYN flood là một kiểu tấn công trực tiếp vào máy chủ bằng cách tạo ra một số lượng lớn các kết nối TCP nhưng không hoàn thành các kết nối này. Phía kẻ tấn công sẽ khởi tạo nhiều TCP, trong mỗi kết nối chỉ để cờ TCP SYN. Máy chủ sẽ gửi lại trả lời vớI TCP SYN và ACK. Nhưng sau đó máy tấn công đơn giản là không trả lời thông điệp thứ ba như mong đợi của server theo tiến trình bắt tay ba chiều. Server lúc này sẽ tốn bộ nhớ và tài nguyên trong khi chờ các phiên TCP timeouts hoặc trước khi các kết nối đang thiết lập dang dở được dọn dẹp. Máy server lúc này có thể từ chối các kết nối TCP khác và các thiết bị cân bằng tải trong các server farm lúc này có thể chia tải không cân bằng. Các firewall có hỗ trợ cơ chế stateful có thể ngăn ngừa kiểu tấn công TCP SYN attack này.

*Sniffing*

Sniffing được hiểu đơn giản là một dạng tấn công bằng cách cố gắng thực hiện việc nghe ngóng các lưu lượng thông tin trên một hệ thống mạng. Tương tự như là thiết bị cho phép nghe lén trên đường dây điện thoại. Chỉ khác nhau ở môi trường là các chương trình Sniffer thực hiện nghe lén trong môi trường mạng máy tính.

Đối tượng thường được Sniffing là các dữ liệu không được mã hóa được truyền trên mạng như: Password (từ Email, Web, SMB, FTP, SQL hoặc Telnet), các thông tin về thẻ tín dụng, văn bản của Email, các tập tin đang di động trên mạng (tập tin Email, FTP hoặc SMB)

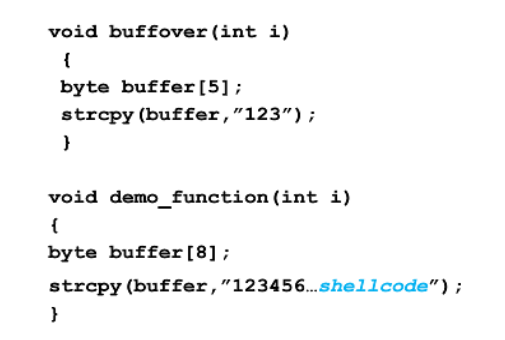
*MITM attack*

Một trong những tấn công mạng thường thấy nhất được sử dụng để chống lại những cá nhân và các tổ chức lớn chính là các tấn công MITM (Man in the Middle). MITM hoạt động bằng cách thiết lập các kết nối đến máy tính nạn nhân và relay các message giữa chúng. Trong trường hợp bị tấn công, nạn nhân cứ tin tưởng là họ đang truyền thông một cách trực tiếp với nạn nhân kia, trong khi đó sự thực thì các luồng truyền thông lại bị thông qua host của kẻ tấn công. Và kết quả là các host này không chỉ có thể thông dịch dữ liệu nhạy cảm mà nó còn có thể gửi xen vào cũng như thay đổi luồng dữ liệu để kiểm soát sâu hơn những nạn nhân của nó.

## Tấn công lớp 7

*Buffer Overflow*

Lỗi tràn bộ đệm (Buffer Overflow) là một điều kiện bất thường khi tiến trình lưu trữ dữ liệu vượt ra ngoài biên của bộ nhớ đệm có chiều dài cố định. Kết quả là dữ liệu có thể đè lên các bộ nhớ liền kề. Dữ liệu bị ghi đè có thể bao gồm các bộ nhớ đệm khác, các biến và dữ liệu điều khiển luồng chảy của cả chương trình (program flow control).

**

*Hình 3.1: Đoạn mã minh họa lỗi Buffer overflow*

Nguyên nhân gây ra lỗi Buffer Overflow của các chương trình, ứng dụng:

- Phương thức kiểm tra bên (boundary) không được thực hiện đầy đủ hoặc là được bỏ qua.

- Các ngôn ngữ lập trình như là ngôn ngữ C, bản thân nó đã tiền ẩn các lỗi mà hacker có thể khai thác.

- Các phương thức strcat(), strcpy(), sprintf(), bcopy(), gets(), canf() trong ngôn ngữ C có thể được khai thác vì các hàm này không kiểm tra những buffer được cấp phát trên stack có kích thước lớn hơn dữ liệu được copy vào buffer hay không. Tác hại của lỗi Buffer Overflow.

- Lỗi tràn bộ đệm xảy ra khi một ứng dụng cố gắng ghi dữ liệu vượt khỏi phạm vi bộ đệm (giới hạn cuối hoặc cả giới hạn đầu của bộ đệm).

- Lỗi tràn bộ đệm có thể khiến ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công kiểm soát hệ thống hoặc tạo cơ hội cho kẻ tấn công thực hiện nhiều thủ thuật khai thác khác nhau.

*Format String*

Tràn bộ đệm chuỗi định dạng (thường được gọi là “lỗ hổng định dạng chuỗi”) là lỗi tràn bộ đệm ở mức chuyên môn cao, tác hại tương tự như các cuộc tấn công tràn bộ đệm khác. Về cơ bản, lỗ hổng định dạng chuỗi tận dụng lợi thế của các kiểu dữ liệu hỗn hợp và kiểm soát thông tin trong chức năng nhất định, chẳng hạn như C/C++ printf



*Hình 3.2: Đoạn mã minh họa lỗi Format String*

Chương trình đơn giản này có đầu vào từ người dùng và hiển thị lại trên màn hình. Chuỗi *%s* có nghĩa là các tham số khác. *str* sẽ được hiển thị như là một chuỗi.

Ví dụ trên không dễ bị tấn công, nhưng nếu thao đổi dòng cuối cùng thành *printf(str);* thì nó có thể dễ dàng bị khai thác.

*Back Door*

Backdoor hay còn gọi là “cổng sau” là chương trình mà hacker cài đặt trên máy tính của nạn nhân để có thể điều khiển hay xâm nhập lại dễ dàng. Một chức năng khác của backdoor là xóa tất cả những thông tin hay các chứng cứ mà hacker có thể để lại khi họ xâm nhập trái phép vào hệ thống, các backdoor tinh vi đôi khi tự nhân bản hay che dấu để có thể duy trì “cổng sau” cho phép các hacker truy cập hệ thống ngay cả khi chúng bị phát hiện. Kỹ thuật mà backdoor thường thực hiện đó là thêm một dịch vụ mới trên các hệ điều hành Windows, và dịch vụ này càng khó nhận dạng thì hiệu quả càng cao. Do đó tên của chúng thường đặt giống với tên của những dịch vụ của hệ thống hay thậm chi các hacker sẽ tìm tên các tiến trình hệ thống nào không hoạt động (hay tắt những tiến trình này) và dùng tên này đặt cho các backdoor của mình. Điều này sẽ qua mặt được cả những chuyên gia hệ thống giàu kinh nghiệm. Một trong các backdoor được sử dụng và chia sẻ phổ biến là Remote Administration Trojan (RAT) cho phép các hacker kiểm soát những máy tính đã bị chiếm quyền điều khiển với những chức năng xem và quản lý toàn bộ desktop, thực thi các tập tin, tương tác vào registry hay thậm chí tạo ra các dịch vụ hệ thống khác. Không như các backdoor thông thường RAT neo chúng và hệ điều hành của nạn nhân để khó bị xóa đi và luôn có hai thành phần trong mô hình hoạt động của backdoor này là thành phần client và thành phần server. Trong đó server là tập tin sẽ được cài vào máy tính bị lây nhiễm còn client là ứng dụng mà các hacker dùng để điều khiển server.

*Sql Injection*

SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp. SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update,… trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy, lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase...

*Xss*

XSS là từ viết tắt của Cross-Site Scripting là một kĩ thuật tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP ...) những thẻ HTML hay những đoạn mã script nguy hiểm. Trong đó những đoạn mã nguy hiểm được chèn vào hầu hết được viết bằng Client-Site Script như javascript, Jscript, DHTML và cũng có thể là các thẻ HTML. XSS là một lỗi phổ biến, mặc dù đã được công bố từ lâu nhưng hiện tại vẫn có rất nhiều trang web bị mắc phải lỗi này.

*File Upload*

Các form upload cho phép người dùng đầu cuối upload file lên trang web các tập tin như hình ảnh, video… Upload file được cho phép trong các ứng dụng mạng xã hội như Facebook và Twitter. Các diễn đàn, blog, Youtube, trang web thương mại điện tử hay cổng hỗ trợ trực tuyến cũng sử dụng tính năng này nhằm cho phép người dùng đầu cuối chia sẻ file với nhân viên công ty. Nhưng do nhiều sai sót trong lập trình trong việc xử lý các tập tin được tải lên máy chủ, khiến cho kẻ tấn công có thể lợi dụng để tải lên những đoạn mã cho phép leo thang và chiếm quyền điểm khiển hệ thống

## Tấn công lớp cao

Các cuộc tấn công dựa trên máy tính truyền thống thường phụ thuộc vào việc tìm kiếm một lỗ hổng trong mã của máy tính. **Social engineering** thì không, kỹ thuật này sử dụng sự ảnh hưởng và sự thuyết phục để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó. Social engineer (người thực hiện công việc tấn công bằng phương pháp social engineering) thường sử dụng điện thoại hoặc internet để dụ dỗ người dùng tiết lộ thông tin nhạy cảm hoặc để có được họ có thể làm một chuyện gì đó để chống lại các chính sách an ninh của tổ chức. Bằng phương pháp này, Social engineer tiến hành khai thác các thói quen tự nhiên của người dùng, hơn là tìm các lỗ hổng bảo mật của hệ thống. Điều này có nghĩa là người dùng với kiến thức bảo mật kém cõi sẽ là cơ hội cho kỹ thuật tấn công này hành động. Các công ty với các phương pháp xác thực, các firewalls, các mạng riêng ảo VPN, các phần mềm giám sát mạng vẫn có rất nhiều khả năng bị tấn công. Một nhân viên có thể vô tình để lộ thông tin key trong email hoặc trả lời điện thoại của một người mà họ không quen biết hoặc thậm chí nói về đề án của họ với đồng nghiệp hàng giờ liền ở quán rượu. Thông thường, mọi người không nhận thấy sai sót của họ trong việc bảo mật, mặc dù họ không cố ý. Những kẻ tấn công đặc biệt rất thích phát triển kĩ năng về Social Engineering và có thể thành thạo đến mức những nạn nhân của không hề biết rằng họ đang bị lừa. Mặc dù có nhiều chính sách bảo mật trong công ty, nhưng họ vẫn có thể bị hại do tin tặc lợi dụng lòng tốt và sự giúp đỡ của mọi người. Những kẻ tấn công luôn tìm những cách mới để lấy được thông tin. Họ chắc chắn là họ nắm rõ vành đai bảo vệ và những người trực thuộc – nhân viên bảo vệ, nhân viên tiếp tân và những nhân viên ở bộ phận hỗ trợ – để lợi dụng sơ hở của họ. Thường thì mọi người dựa vào vẻ bề ngoài để phán đoán. Ví dụ, khi nhìn thấy một người mặc đồng phục màu nâu và mang theo nhiều hộp cơm, mọi người sẽ mở cửa vì họ nghĩ đây là người giao hàng. Hay khi bạn nhặt được một chiếc USB bạn có thể rất vô tư cắm nó ngay vào máy tính để xem nó là của ai và chứa thông tin gì. Nhưng đó có thể chính là nguồn phát tán virus và mã độc đến bạn, tổ chức và người thân của bạn. Một số công ty liệt kê danh sách nhân viên trong công ty kèm theo số điện thọai, email trên Website của công ty. Ngoài ra, các công ty còn thêm danh sách các nhân viên chuyên nghiệp đã được đào tạo trong cơ sở dữ liệu Oracle hay UNIX servers. Đây là một số ít thông tin giúp cho attacker biết được loại hệ thống mà họ đang định xâm nhập.

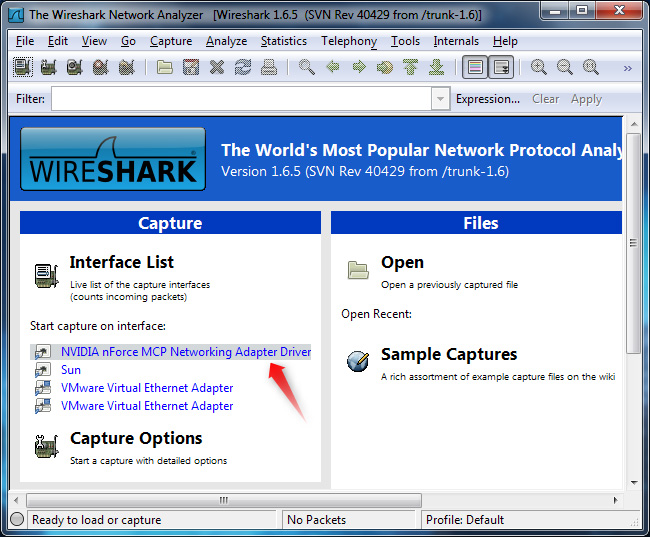
## Kỹ năng phân tích tấn công.

**Phân tích gói tin**

Phân tích gói tin thông thường được quy vào việc nghe các gói tin và phân tích giao thức, mô tả quá trình bắt và phiên dịch các dữ liệu sống như là các luồng đang lưu chuyển trong mạng với mục tiêu hiểu rõ hơn điều gì đang diễn ra trên mạng. Phân tích gói tin thường được thực hiện bởi một packet sniffer, một công cụ được sử dụng để bắt dữ liệu thô đang lưu chuyển trên đường dây. Phân tích gói tin có thể giúp chúng ta hiểu cấu tạo mạng, ai đang ở trên mạng, xác định ai hoặc cái gì đang sử dụng băng thông, chỉ ra những thời điểm mà việc sử dụng mạng đạt cao điểm, chỉ ra các khả năng tấn công và các hành vi phá hoại, và tìm ra các ứng dụng không được bảo mật.

Để thực hiện việc bắt các gói tin trên mạng, ta phải chỉ ra những vị trí tương ứng để đặt “máy nghe” vào hệ thống đường truyền của mạng. Quá trình này đơn giản là đặt “máy nghe” vào đúng vị trí vật lý nào trong một mạng máy tính. Việc nghe các gói tin không đơn giản chỉ là cắm một máy xách tay vào mạng và bắt gói. Thực tế, nhiều khi việc đặt máy nghe vào mạng khó hơn việc phân tích các gói tin. Thách thức của việc này là ở chỗ là có một số lượng lớn các thiết bị mạng phần cứng được sử dụng để kết nối các thiết bị với nhau. Lý do là vì 3 loại thiết bị chính (hub, switch, router) có nguyên lý hoạt động rất khác nhau. Và điều này đòi hỏi ta phải nắm rõ được cấu trúc vật lý của mạng mà ta đang phân tích.

Có rất nhiều công cụ hỗ trợ phân tích gói tin, phổ biến nhất trong số đó là Wireshark. Đây là công cụ có khả năng theo dõi, giám sát các gói tin theo thời gian thực, hiển thị chính xác báo cáo cho người dùng qua giao diện khá đơn giản và thân thiện.



Hình 3.3: Công cụ Wireshark

**Phân tích Log file hệ thống**

Mỗi hệ thống điều duy trì ghi log có thể cung cấp các thông tin. Điều quan trọng là có thể tìm kiếm các bản ghi bằng chứng ấy. Bản ghi log hệ thống thường chỉ ra đăng nhập thất bại hay thành công, cũng như bất kỳ cảnh báo mà hệ điều hành đưa ra. Sự khác nhau của các phiên bản Windows Server cũng ghi lại mỗi lần khởi động trong nhật ký. Vì vậy khi điều tra, chúng ta có thể nhìn vào bản ghi log trong một vài hệ điều hành để tìm ra những thông tin hữu ích.

Với Windows XP/Vista/7. Trong tất cả các phiên bản của Windows, ta có thể tìm thấy các bản ghi log bằng cách nhấp vào nút Start ở góc dưới bên trái của màn hình, sau đó nhấp vào Control Panel. Sau đó click vào Administrator Tools và Event Viewer. Ta thấy Event Viewer thể hiện trong hình 3.6. Bây giờ từ màn hình này ta có thể xem bản ghi log và các sự kiện. Nếu xem xét một phiên bản của Windows trước XP, một số log sau có thể không có mặt :

* **Bản ghi log ứng dụng** : ghi lại nhiều sự kiện đăng nhập bởi các ứng dụng. Nhiều ứng dụng sẽ ghi lại lỗi của chúng ở đây trong bản ghi log ứng dụng. Điều này có thể hữu ích đặc biệt là nếu đăng nhập trên một máy chủ mà có cơ sở dữ liệu.
* **Bản ghi log bảo mật** : Điều quan trọng nhất có thể tìm thấy trong bản ghi log bảo mật là lần đăng nhập thành công và lỗi. Bản ghi này cũng ghi lại các sự kiện liên quan đến sử dụng tài nguyên, như tạo, mở, hoặc xóa các tập tin hoặc đối tượng khác. Các quản trị viên có thể xác định những sự kiện được ghi lại trong bản ghi log bảo mật. Một số hacker/cracker tắt bản ghi log bảo mật để hoạt động của chúng không được ghi lại.
* **Bản ghi log Setup** : chứa các sự kiện liên quan đến cài đặt ứng dụng. Nơi này sẽ hiển thị các ứng dụng mới được cài đặt trên máy. Rõ ràng, hầu hết các virus và phần mềm gián điệp sẽ không ghi tới bản ghi log ứng dụng. Tuy nhiên, bản ghi này có thể cho biết các ứng dụng mới đã được cài đặt mà có thể là một lỗ hổng bảo mật hoặc là trojan.
* **Bản ghi log hệ thống**: Có chứa các sự kiện đăng nhập bởi các thành phần hệ thống Windows. Điều này bao gồm các sự kiện như lỗi driver.
* **Bản ghi sự kiện chuyển tiếp**: Được sử dụng để lưu trữ các sự kiện thu thập được từ máy tính từ xa. Nhật ký này rất quan trọng trong một môi trường mạng. Tuy nhiên, các hệ thống khác nhau phải được cấu hình để có được bản ghi này.
* **Bản ghi các ứng dụng và dịch vụ**: Là một loại bản ghi mới của bản ghi log sự kiện. Những sự kiện này lưu trữ các bản ghi từ một ứng dụng hoặc thành phần chứ không phải là sự kiện có tác động lên toàn hệ thống. Điều này có tiết lộ các vấn đề với một ứng dụng cụ thể hoặc thành phần Windows.

Hai bản ghi log quan trọng là bảo mật và đăng nhập hệ thống. Các hạng mục quan trọng nhất trong bản ghi log bảo mật là bản ghi của tất cả các đăng nhập hoặc đăng xuất dù là thành công hay không thành công. Đây là dấu hiệu đầu tiên của một nỗ lực xâm nhập vào máy chủ. Nếu thấy rất nhiều lần đăng nhập thất bại, hoặc nếu thấy thông tin đăng nhập tài khoản vào các giờ lẻ, mà có thể là một dấu hiệu cho thấy hoạt động bất hợp pháp đang diễn ra. Đây là một trong những điều đơn giản nhất để kiểm tra, vì vậy chắc chắn không nên bỏ qua phần này.

Hệ điều hành Linux cũng ghi lại nhật ký hoạt động.Tất cả các bản ghi log hệ thống điều hành có thể tìm được trong mục /var/log subdirectory. Có một số bản ghi log có thể tìm thấy trong thư mục này. Một vài trong số này không có mặt trong tất cả các bản của Linux, vậy cần tìm trong thư mục đó và xem các bản ghi log có mặt:

* /var/log/faillog: tập tin đăng nhập này có chứa thông tin đăng nhập người dùng không thành công. Điều này có thể rất quan trọng khi theo dõi cracker.
* /var/log/kern.log: tập tin đăng nhập này được sử dụng cho tất cả các tin nhắn từ nhân của hệ điều hành. Điều này không có khả năng thích hợp với hầu hết các máy tính của tội phạm.
* /var/log/lpr.log: đây là nhật ký log máy in có thể cung cấp một bản ghi bất kỳ được in ra từ máy này. Điều này có thể hữu ích cho doanh nghiệp cạnh tranh.
* /var/log/mail.\*: đây là nhật ký máy chủ email và có thể hữu ích trong việc điều tra tội phạm máy tính. Email có thể là một phần cần thiết của bất kỳ tội phạm máy tính nào .
* /var/log/mysql.\*: bản ghi log này liên quan đến hồ sơ máy chủ cơ sở dữ liệu MySql .
* /var/log/apache2/\*: nếu máy tính này đang chạy máy chủ web Apache, sau đó bản ghi log sẽ hiển thị các hoạt động liên quan. Điều này hữu ích khi theo dõi hacker.
* /var/log/lighttpd/\*: nếu máy này đang chạy máy chủ web Lighttpd, sau đó bản ghi log sẽ hiển thị các hoạt động liên quan. Điều này có thể hữu ích khi theo dõi hacker cố gắng hack máy chủ web.
* /var/log/apport.log: Đây là hồ sơ ứng dụng bị treo. Đôi khi, nó cho thấy sự hiện diện của virus hoặc phần mềm gián điệp.
* /var/log/user.log: Chứa bản ghi hoạt động của người dùng và có thể rất quan trọng với một cuộc điều tra hình sự.

Có một số phương pháp để xem các bản ghi, trong đó có một số lệnh ai cũng có thể vào và xem các bản ghi trong hệ thống linux. Ví dụ nếu muốn xem nhật ký ghi log máy in, làm như sau :

* # tail –f/var/log/lbr.log
* # less/var/log/lbr.log
* # more –f/var/log/lbr.log
* # vi/var/log/lbr.log

Tuy nhiên, bằng cách sử dụng lệnh dmesg trong Linux có thể xem các bản ghi từ vỏ. : dmesg | lpr

Nhưng một số bản ghi log chỉ có quyền root mới được xem. Nếu sử dụng giao diện người dùng đồ họa Gnome, nó đi kèm với một tiện ích có tên là System Log Viewer. Tiện ích này là một đồ họa, xem trình đơn điều khiển có thể sử dụng xem tất cả các bản ghi log của hệ thống. Hệ thống Log Viewer đi kèm với xây dựng các chức năng như lịch, màn hình đăng nhập và hiển thị số liệu thống kê. Đây là một công cụ rất hữu ích cho việc kiểm tra các bản ghi hệ thống Linux.

# Phần mềm mã độc

## Tổng quan phần mềm mã độc.

Malware (Malicious software) hay còn gọi là mã độc hại (Maliciuos code) là tên gọi chung cho các phần mềm được thiết kế, lập trình đặc biệt để phá hoại hệ thống của bạn hoặc làm gián đoạn môi trường hoạt động mạng. Malware thâm nhập vào một hệ thống máy tính mà không có sự đồng ý của chủ sở hữu.

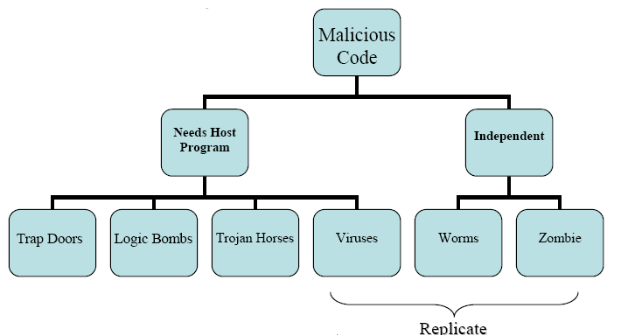
Sự gia tăng đột biến của các mã độc hại (malware) trong những năm gần đây là dấu hiệu rất đáng lo ngại cho các tổ chức, người dùng máy tính. Mục tiêu mà tin tặc nhắm đến là các mạng xã hội vốn đang được cư dân mạng sử dụng rất nhiều. Các chương trình mã độc hại ngày càng phức tạp và nguy hiểm, nhưng cũng có chương trình lại rất đơn giản xét từ góc độ kỹ thuật, và lại rất phổ biến. Tuy nhiên, các chương trình phức tạp và nguy hiểm lại tăng lên nhiều so với 4 năm trước đây, trong đó nguy hiểm nhất là những chương trình có khả năng tự nhân bản, giữ nguyên các tính năng phá hoại và đồng thời sử dụng những cách thức che dấu sự hiện diện của mình trong hệ thống. Bản thân công nghệ được sử dụng để lẩn tránh của mã độc hại là rất mới và tinh vi. Cách đây 4-5 năm, công nghệ tự che dấu như vậy vẫn còn trong giai đoạn nghiên cứu, nhưng hiện nay chúng đã trở thành dịch toàn cầu. Công nghệ tự nhân bản thì tuy đã có cách đây 20 năm và về nguyên lý thì công nghệ này khong có gì thay đổi cho đến nay. Tuy nhiên, khả năng tự nhân bản hiện nay thường kết hợp với những công nghệ khác để tạo ra khả năng lây lan và phá hoại hiệu quả hơn rất nhiều.

Sự phát triển của các mạng xã hội sẽ tạo ra môi trường tốt cho các chương trình độc hại. Điều này có thể lí giải đơn giản: người dùng tỏ ra tin tưởng các thành viên trong mạng xã hội hơn, và do đó cũng không e ngại hoặc ít đề phòng hơn so với những cách thức giao tiếp khác. Mặt khác, mạng xã hội quy tụ rất nhiều thành phần, và trình độ nhận thức, hiểu biết về an toàn, bảo mật của người dùng trong mạng cũng rất thấp. Từ đó, có thể thấy rằng các chương trình độc hại tìm được môi trường rất phù hợp trong mạng xã hội.

Sự phát triển của các dòng điện thoại thông minh cũng là môi trường cho các hacker phát tán mã độc hại với mục đích chủ yếu nhằm ăn cắp thông tin người dùng. Thị trường điện thoại di động ngày càng được các hacker chú ý đến.

## Phân loại mã độc hại

Có nhiều tiêu chí để phân loại mã độc hại, dưới đây là cách phân loại dựa vào hình thức lây nhiễm, sự chỉ phân loại mang tính chất tương đối.



*Hình 4.1: Phân loại mã độc hại*

Theo hình trên mã độc hại gồm 2 loại chính: một loại cần vật chủ để tồn tại và lây nhiễm, vật chủ ở đây có thể là các file dữ liệu, các file ứng dung, hay các file chương trình thực thi… và một loại là tồn tại độc lập.

Độc lập nghĩa là đó là chương trình độc hại mà có thể được lập lịch và chạy trên hệ điều hành.

Không độc lập (needs host program) là 1 đoạn chương trình đặc biệt thuộc 1 chương trình nào đó không thể thực thi độc lập như một chương trình thông thường hay tiện ích nào đó mà bắt buộc phải có bước kích hoạt chương trình chủ trước đó thì chương trình đó mới chạy.

**Trap Door**

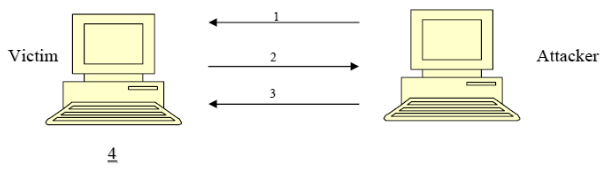
Trap Door còn được gọi là Back Door là một điểm bí mật trong một chương trình, cho phép một ai đó có thể truy cập lại hệ thống mà không phải vượt qua các hàng rào an ninh như thông thường. Trap door được sử dụng bởi những nhà lập trình với mục đích dò lỗi, kiểm tra chương trình. Trong các cuộc tấn công trap door là phần mềm độc hại thường trú và đợi lệnh điều khiển từ các cổng dịch vụ TCP hoặc UDP. Trap door khi chạy trên máy bị nhiễm, nó sẽ thường trược trong bộ nhớ và mở một cổng cho phép kẻ tấn công truy nhập vào máy nạn nhân thông qua cổng mà nó đã mở và kẻ tấn công có toàn quyền điều khiển máy bị nhiễm.

Trap door nguy hiểm ở chỗ nó hoàn toàn chạy ẩn trong máy. Nhiều con được hẹn trước giờ để kết nối ra ngoài (đến 1 giờ nhất định mới mở 1 port để hacker đột nhập vô) nên rất khó phát hiện ngay cả scan port.

**Logic Bombs**

Logic bomb là đoạn mã độc được nhúng vào một chương trình hợp pháp mà chúng có thể thực thi khi có một sự kiện nào đó xảy ra. Các đoạn mã thường được chèn vào các ứng dụng hoặc các hệ điều hành để thực hiện việc phá hủy hệ thống hoặc phá hủy các chức năng an toàn của hệ thống.

Logic bomb có thể gửi thông báo tới kẻ tấn công khi người dùng truy nhập Internet và sử dụng một chương trình đặc biệt nào đó như bộ xử lý văn bản. Từ đó attacker có thể chuẩn bị cho các cuộc tấn công (chẳng hạn kết hợp với các máy tính khác bị nhiễm để bắt đầu một cuộc tấn công từ chối dịch vụ).



*Hình 4.2: Mô hình hoạt động Logic bomb*

**Trojan Horses**

Trojan Horse là loại mã độc hại được đặt theo sự tích “Ngựa thành Troy”. Trojan horse không có khả năng tự nhân bản tuy nhiên nó lây vào hệ thống với biểu hiện rất bình thường nhưng thực chất bên trong có ẩn chứa các đoạn mã với mục đích gây hại. Trojan có thể gây hại theo ba cách sau:

Tiếp tục thực thi các chức năng của chương trình mà nó bám vào, bên cạnh đó thực thi các hoạt động gây hại một cách riêng biệt (ví dụ như gửi một trò chơi dụ cho người dùng sử dụng, bên cạnh đó là một chương trình đánh cắp password).

Tiếp tục thực thi các chức năng của chương trình mà nó bám vào, nhưng sửa đổi một số chức năng để gây tổn hại (ví dụ như một trojan giả lập một cửa sổ login để lấy password) hoặc che dấu các hành động phá hoại khác (ví dụ như trojan che dấu cho các tiến trình độc hại khác bằng cách tắt các hiển thị của hệ thống).

Thực thi luôn một chương trình gây hại bằng cách núp dưới danh một chương trình không có hại (ví dụ như một trojan được giới thiệu như là một chò chơi hoặc một tool trên mạng, người dùng chỉ cần kích hoạt file này là lập tức dữ liệu trên PC sẽ bị xoá hết).

Có 7 loại trojan chính:

*Trojan truy cập từ xa:* Được thiết kế để cho kẻ tấn công có khả năng từ xa chiếm quyền điều khiển của máy bị hại. Các trojan này thường dấu vào các trò chơi và các chương trình nhỏ làm cho người dùng mất cảnh giác.

*Trojan gửi dữ liệu:* Nó thực hiện việc lấy và gửi dữ liệu nhạy cảm như mật khẩu, thông tin thẻ tín dụng, các tệp nhật ký, địa chỉ email… cho kẻ tấn công. Trojan này có thể tìm kiếm cụ thể thông tin hoặc cài phần mềm đọc trộm bàn phím và gửi toàn bộ các phím bấm về cho kẻ tấn công.

*Trojan hủy hoại:* Thực hiện việc xóa các tệp tin. Loại trojan này giống với virus và thường có thể bị phát hiện bởi các chương trình diệt virus.

*Trojan kiểu proxy:* Sử dụng máy tính bị hại làm proxy, qua đó có thể sử dụng máy bị hại để thực hiện các hành vi lừa gạt hay đánh phá các máy tính khác.

*Trojan FTP:* Được thiết kế để mở cổng 21 và cho phép tin tặc kết nối vào máy bị hại sử dụng FTP.

*Trojan tắt phần mềm an ninh:* Thực hiện việc dừng hoặc xóa bỏ chương trình an ninh như phần mềm chống virus hay tường lửa mà người dùng không nhận ra.

*Trojan DoS:* Được sử dụng trong các cuộc tấn công từ chối dịch vụ. Ví dụ các con bot sử dụng trong DDoS cũng có thể coi là một loại trojan.

**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 lây lan. Các chương trình diệt virus dựa vào đặc tính này để thực thi việc phòng chống và diệt virus, để quét các file trên các thiết bị lưu trữ, quét các file trước khi lưu xuống ổ cứng. Vì vậy đôi khi các phần mềm diệt virus tại PC đưa thông báo “phát hiện nhưng không diệt được” khi thấy có các dấu hiệu hoạt động của virus trên PC vì “vật mang virus” lại nằm trên một máy khác nên không thể thực thi việc xóa đoạn mã độc đó.

Virus có thể làm bất cứ việc gì mà các chương trình khác có thể làm. Virus chỉ khác ở điểm nó tự đính kèm nó tới một chương trình và thực thi bí mật khi chương trình mang Virus được thực thi. Khi virus được thực thi nó có thể làm bất kỳ việc gì trên hệ thống như xóa file, chương trình. Vòng đời virus gồm 4 giai đoạn:

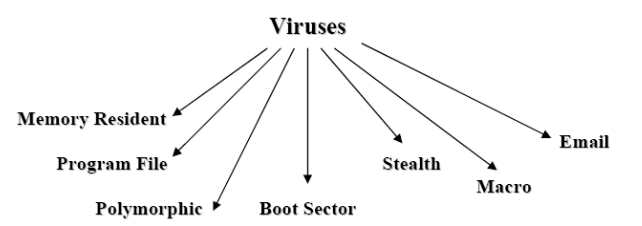
*Dormant (nằm im):* Trong giai đoạn này Virus không làm gì cho đến khi được kích hoạt bởi một ai đó hay một sự kiện nào đó.

*Propagation (lây lan):* Trong giai đoạn này virus thực hiện việc copy chính nó tới các chương trình, vị trí khác trong ổ đĩa.

*Triggering:* Trong giai đoạn này virus được kích hoạt để thực thi chức năng của nó.

*Execution:* Chức năng của virus được thực thi. Chức năng có thể là vô hại như gửi một thông điệp nào đó tới màn hình, hoặc một chức năng có hại như phá hủy các chương trình, các file hệ thống.

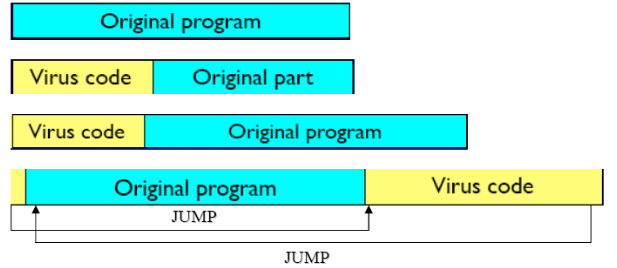
Virus gồm 7 loại chính



Hình 4.3 Phân loại virus

*Memory – resident virus:* Cư trú rong bộ nhớ chính như là một phần của chương trình hệ thống. Theo đó virus sẽ gây ảnh hưởng mỗi khi chương trình được thực thi.

*Program file virus:* Gây ảnh hưởng đến các file chương trình như exe/com/sys.



Hình 4.4: Mô tả virus lây file

*Polymorphic virus( Virus đa hình):* Loại Virus này tự thay đổi hình thức của nó, gây khó khăn cho các chương trình anti-virus. Virus “Tequilla” là loại virus đa hình đầu tiên xuất hiện năm 1991.

*Boot Sector virus:* Là loại Virus đầu tiên trên thế giới được phổ biến rộng rãi và được viết vào năm 1986. Boot Virus lợi dụng tiến trình boot của máy tính để thực hiện việc kích hoạt mình. Khi máy tính được khởi động, nó luôn tìm đến master boot record được lưu trữ tại địa chỉ head 0, track 0, sector 1 để đọc thông tin. Boot Sector virus lây lan sang đĩa cứng khi khởi động hệ thống từ đĩa mềm bị nhiễm.

*Stealth virus:* Đây là loại virus có khả năng tự che dấu không để cho hệ điều hành và phần mềm chống virus biết. Nó nằm trong bộ nhớ để ngăn chặn sử dụng hệ điều hành và che dấu những thay đổi về kích thước các tập tin. Những virus này chỉ bị phát hiện khi chúng còn ở trong bộ nhớ. Có nhiều boot sector virus có khả năng Stealth. Ví dụ virus "The Brain” được tạo ra tại Pakistan bởi Basit và Amjad. Chương trình này nằm trong phần khởi động (boot sector) của một đĩa mềm 360Kb và nó sẽ lây nhiễm tất cả các ổ đĩa mềm. Đây là loại "stealth virus" đầu tiên.

*Macro virus:* Là tập lệnh được thực thi bởi một ứng dụng nào đó. Macro virus phổ biến trong các ứng dụng Microsoft Office khi tận dụng khả năng kiểm soát việc tạo và mở file để thực thi và lây nhiễm. Ví dụ: virus Baza, Laroux và một số virus Staog xuất hiện năm 1996 tấn công các file trong hệ điều hành Windows 95, chương trình bảng tính Excel và cả Linux.

Virus Melisa cũng là một trong những Macro virus nổi tiếng.

*Email virus:* Là những virus được phát tán qua thư điện tử. Ví dụ virus Melissa được đính kèm trong thư điện tử. Nếu người dùng mở file đính kèm Macro được kích hoạt sau đó email virus này tự động gửi chính nó tới tất cả những hòm thư có trong danh sách thư của người đó.

**Worms**

Worm là chương trình độc hại có khả năng tự nhân bản và tự lây nhiễm trong hệ thống mà không cần file chủ để mang nó khi nhiễm vào hệ thống. Như vậy Worm không bám vào một file hoặc một vùng nào đó trên đĩa cứng, vì vậy không thể dùng các chương trình quét file để diệt Worm. Mục tiêu của Worm là làm lãng phí băng thông của mạng, phá hoại hệ thống như xóa file, tạo back door, thả keylogger…

Tấn công của Worm có đặc trưng là lan rộng cực kỳ nhanh chóng do không cần tác dụng của con người( như khởi động máy, copy file hay đóng/mở file).

Worm có thể chia làm 2 loại:

Network Service Worm lan truyền bằng cách lợi dụng các lỗ hổng bảo mật của mạng, của hệ điều hành hoặc của ứng dụng.

Mass Mailing Worm là một dạng tấn công qua dịch vụ mail, tuy nhiên nó tự đóng gói để tấn công và lây nhiễm chứ không bám vào vật chủ là email. Khi sâu này lây nhiễm vào hệ thống, nó thường cố gắng tìm kiếm sổ địa chỉ và tự gửi bản thân nó đến các địa chỉ thu nhặt được. Việc gửi đồng thời cho toàn bộ các địa chỉ thường gây quá tải cho mạng hoặc cho máy chủ mail.

**Zombie**

Zombie là chương trình độc hại bí mật liên kết với một máy tính khác ngoài internet để nghe lệnh từ các máy tính đó. Các Zombie thường sử dụng trong các cuộc tấn công từ chối dịch vụ DDoS để tấn công vào một website nào đó.

Kiểu thông dụng nhất của Zoombie là các agent dùng để tổ chức một cuộc tấn công DDoS. Kẻ tấn công có thể cài Zoombie vào một số lượng lớn các máy tính rồi ra lênh tấn công cùng một lúc.

## Dấu hiệu hệ thống mạng, máy tính của mình bị nhiễm mã độc hại

Dấu hiệu nhiễm Virus :

* Hệ thống tự động shutdown hoặc logging off đột ngột.
* Hệ thống có ít memory hơn bình thường.
* Tên một ổ đĩa bị thay đổi hay không có thể truy cập được vào.
* Các chương trình và các files đột nhiên không truy cập được vào (ví dụ Task manager, Registry Editor, Folder Options).
* Các chương trình hoặc files lạ thường được tạo ra.
* Lưu lượng mạng trong hệ thống tăng cao.

Dấu hiệu nhiễm Trojan :

* Màn hình tự dưng có gợn sóng.
* Wall paper của máy bị thay đổi.
* Màu sắc cửa sổ Windows bị thay đổi.
* Chức năng chuột trái, chuột phải bị hoán đổi vị trí lẫn nhau.
* Con trỏ chuột không xuất hiện.
* Con trỏ chuột tự di chuyển.
* Nút Windows Start không xuất hiện.
* Thanh Taskbar tự dưng không xuất hiện.
* Máy tính bạn tự dưng shutdown hoặc tự tắt.

Dấu hiệu nhiễm Spyware

* Tự động Spyware thay đổi trang web mặc định, khi bạn nhấn vào nút home sẽ ra trang mà spyware ấn định sẵn.
* Firewall và các chương trình antivirus tự động tắt.
* Đèn báo mạng của bạn sáng nhấp nháy nhiều, trong khi bạn không làm gì trên Internet.
* Không thể tắt được hết các popup windows nhảy ra.
* Bạn thấy 1 chương trình mới trong mục add/remove program mà trước đó bạn chưa bao giờ cài.
* Có 1 vài icon và shortcuts lạ nằm trên thành taskbar của bạn, system tray hoặc trên desktop của bạn.
* Bạn chuyển tới 1 một trang lạ thay vì lỗi 404 error, khi trang web không tìm thấy.
* Bạn nhận cảnh báo liên tục từ firewall của bạn về một chương trình không rõ ràng hoặc một tiến trình nào đó cố gắng truy cập ra Internet.
* Bạn nhận được một số email quay trở lại hoặc nhìn thấy có một số email tự gửi đi mà không phép của bạn.
* Trình duyệt web của bạn chạy chậm hơn so với bình thường.
* Có thanh toolbar xuất hiện lạ thường trên web-browser và bạn không biết nó cài vào máy bạn từ bao giờ.
* …..

Nhìn chung dấu hiệu nhận biết máy mình nhiễm mã độc hại thì có nhiều, thường chúng ta tham khảo các trang web về bảo mật, về mã độc hại để xem các triệu chứng, xem có giống máy mình không

## Các phương pháp phân tích mã độc hại

Phương pháp phân tích thì có 2 phương pháp chính :

* Dynamic analysis (phân tích hành vi mã độc hại).
* Static analysis (phân tích mã độc hại bằng cách xem mã dịch ngược của mã độc hại).

**Static analysis**

Static analysis thì mình sẽ xem code để xem thực sự mã độc hại này sẽ làm gì trên hệ thống. Không cần phải chạy mã độc hại đó, và hiểu rõ hơn thực sự về hoạt động của malware. Các công cụ thường sử dụng trong quá trình phân tích tĩnh có thể kể đến các chương trình dịch ngược :

* Disassembler
* Decompiler
* Source Code Analyzer

*Ưu điểm :*

Static analysis là có thể phát hiện ra hoạt động, cách ứng xử của chương trình trong những điều kiện không tồn tại thực tế.

Static analysis sẽ cho chúng ta cái nhìn rất đúng nhất về một chương trình. Sở dĩ gọi là gần đúng bởi rất hiếm khi chúng ta có thể nắm được toàn bộ hoạt động của một chương trình, trừ các chương trình đủ nhỏ.

*Nhược điểm :*

Phương pháp này đòi hỏi người phân tích phải am hiểu sâu về hệ thống và lập trình.

**Dynamic analysis**

Dynamic analysis thì là quan sát xem mã độc hại khi thực thi thì sẽ làm những gì, nó chạy ra sao, làm gì trên máy tính mình qua các công cụ monitor, cách này thì có nhược điểm với các dòng mã độc hại chạy theo lịch trình. Nghiên cứu hoạt động của chương trình bằng cách thực thi chương trình đó. Các công cụ được sử dụng trong trường hợp này có thể kể đến như :

* Debugger
* Function call tracer
* Machine emulator
* Logic analyzer
* Network sniffer

*Ưu điểm :*

Dynamic analysis thì nhanh và thông tin chính xác. Tuy nhiên dynamic analysis có một khuyết điểm là: "Tất cả những thấy không phải là tất cả những gì chương trình có". Nói cách khác dynamic analysis không thể dự đoán được những hành vi của chương trình trong các điều kiện "đặc biệt" không tồn tại trong thực tế. Có thể lấy ví dụ với các mã độc hại chạy theo thời gian, tức là ở thời điểm này mình cho nó chạy nó không có hoạt động gì, nhưng ở một thời điểm khác nó lại chạy.

Mỗi phương pháp đều có một đặc điểm riêng nhưng khi phân tích mã độc hại thì người ta thường phải sử dụng cả 2 phương pháp để hỗ trợ lẫn nhau:

Dù mục đích chính thì giống nhau nhưng các công cụ hỗ trợ việc phân tích, thời gian bỏ ra của từng phương pháp là khác nhau.

## Xây dựng giải pháp phòng và chống phần mềm mã độc

Việc ngăn ngừa, phòng chống mã độc hại có thể dựa trên một số biện pháp sau:

**Xây dựng chính sách bảo đảm an toàn:**

Chính sách của các tổ chức cần giải quyết được vấn đề phòng, chống và xử lý các sự cố liên quan tới phần mềm độc hại. Nội dung của chính sách nên được sử dụng làm cơ sở cho những nỗ lực phòng - chống phần mềm độc hại một cách nhất quán và hiệu quả trong toàn bộ tổ chức. Chính sách phải mang tính tổng quát, có thể linh hoạt trong việc thực hiện chính sách và làm giảm nhu cầu cập nhật chính sách thường xuyên, nhưng cũng phải cụ thể để thực hiện mục đích và phạm vi của chính sách rõ ràng. Chính sách liên quan đến công tác phòng - chống phần mềm độc hại phổ biến bao gồm:

- Yêu cầu quét phần mềm độc hại trên các phương tiện thông tin từ bên ngoài đưa vào tổ chức trước khi sử dụng chúng.

- Yêu cầu các tập tin đính kèm email phải được quét virus trước khi chúng được mở ra.

- Cấm gửi hoặc nhận một số loại tập tin giống như các tập tin .exe qua email.

- Hạn chế hoặc cấm sử dụng phần mềm không cần thiết, như các tin nhắn mang danh cá nhân và dịch vụ chia sẻ hồ sơ tức thời.

- Hạn chế việc sử dụng các phương tiện lưu trữ di động (các ổ đĩa flash…), đặc biệt là trên các máy chủ có nguy cơ lây nhiễm cao, các trạm truy cập mạng công cộng….

- Chỉ rõ các loại phần mềm phòng ngừa (chống virus, lọc nội dung) bắt buộc đối với từng loại máy tính (máy chủ email, máy chủ web, máy tính xách tay, điện thoại thông minh) và ứng dụng (ứng dụng email, trình duyệt web), cùng danh sách các yêu cầu nâng cao cho cấu hình và bảo trì phần mềm (như tần suất cập nhật phần mềm, tần suất và phạm vi quét máy chủ).

- Hạn chế hoặc cấm sử dụng thiết bị di động của tổ chức hoặc của cá nhân kết nối với mạng của tổ chức cho việc truy cập từ xa.

**Sử dụng phần mềm ngăn chặn mã độc**

Cách hiệu quả nhất để ngăn chặn phần mềm độc hại là cài đặt phần mềm chống virus cho máy tính. Chương trình chống virus sẽ bảo vệ máy tính trước sự tấn công của tin tặc, virus, phần mềm độc hại, phần mềm gián điệp, trojan... Một số chương trình chống virus cũng sẽ tối ưu hóa hiệu suất máy tính, tự động sao lưu các tập tin. Hiện nay, trên thị trường có nhiều nhà sản xuất phần mềm bảo mật máy tính như Symantec, McAfee….

**Nâng cao nhận thức của người dùng**

Các chương trình nâng cao nhận thức nên bao gồm hướng dẫn cho người dùng về cách phòng ngừa sự cố phần mềm độc hại để có thể góp phần làm giảm tần suất và mức độ nghiêm trọng của sự cố phần mềm độc hại. Chương trình nâng cao nhận thức của tổ chức nên bao gồm những yếu tố phòng ngừa sự cố phần mềm độc hại được nêu trong các chính sách và thủ tục của tổ chức. Một số nội dung thực tế cần tuân thủ như sau:

+ Không mở các email đáng ngờ hoặc file đính kèm email, kích chuột vào siêu liên kết nghi ngờ, hoặc truy cập các trang web có thể chứa nội dung độc hại.

+ Không kích chuột vào trình duyệt web, cửa sổ popup nghi ngờ độc hại.

+ Không mở các tập tin với phần mở rộng như .Bat, .com, .exe, .pif, .vbs, thường có nhiều khả năng được liên kết với các phần mềm độc hại.

+ Không vô hiệu hóa các cơ chế kiểm soát an ninh, phần mềm độc hại (như phần mềm chống virus, phần mềm lọc nội dung, tường lửa cá nhân).

+ Các Host bình thường không được sử dụng tài khoản cấp cho quản trị viên.

+ Không tải hoặc thực hiện các ứng dụng từ các nguồn không tin cậy.

Người dùng cũng cần biết về chính sách và thủ tục áp dụng để xử lý sự cố phần mềm độc hại, chẳng hạn như cách thức để xác định một máy chủ bị nhiễm phần mềm độc hại, cách báo cáo một nghi ngờ có sự cố, để hỗ trợ xử lý sự cố. Người sử dụng cũng cần được biết về cách thức thông báo sự cố phần mềm độc hại chính và đưa ra cách để xác minh tính xác thực của tất cả các thông báo. Ngoài ra, người sử dụng cần phải biết thực hiện một số thao tác khi có sự cố, chẳng hạn như ngắt kết nối máy chủ bị nhiễm phần mềm độc hại từ các mạng.

**Đối phó với loại tấn công sử dụng kỹ nghệ xã hội**

Mọi người dùng có thể nhận thức được vai trò của mình trong việc ngăn ngừa sự cố, nhằm tránh các loại tấn công dựa trên kỹ nghệ xã hội. Các khuyến nghị để tránh các cuộc tấn công lừa đảo và các hình thức kỹ nghệ xã hội bao gồm:

+ Không bao giờ trả lời email yêu cầu thông tin tài chính hoặc cá nhân. Thay vào đó, liên lạc với người hoặc tổ chức tại số điện thoại hoặc trang web hợp pháp. Không sử dụng thông tin liên hệ cung cấp trong email và không bấm vào bất kỳ file đính kèm hoặc các siêu liên kết trong email nghi ngờ.

+ Không cung cấp mật khẩu, mã PIN hoặc mã truy cập khác để đáp ứng với các email từ địa chỉ lạ hoặc cửa sổ mới. Chỉ nhập thông tin vào các trang web hoặc ứng dụng hợp pháp.

+ Không mở tập tin đính kèm email đáng ngờ, ngay cả khi chúng đến từ những người gửi đã quen biết. Nếu nhận được một tập tin đính kèm bất ngờ, cần liên hệ với người gửi (tốt nhất là bằng một phương pháp khác ngoài email, chẳng hạn như điện thoại) để xác nhận rằng tập tin đính kèm là hợp pháp.

+ Không trả lời bất kỳ email đáng ngờ hoặc từ địa chỉ lạ.

Trong Bản hướng dẫn, NIST cũng khuyến cáo các tổ chức/doanh nghiệp cần xây dựng kế hoạch và thực hiện chương trình phòng ngừa sự cố từ phần mềm độc hại dựa trên phân tích các rủi ro theo hướng tổng hợp tất cả các cuộc tấn công đối với hệ thống mạng. Các biện pháp phòng ngừa phải khoa học, phù hợp với quy mô, cấu trúc mạng để bảo vệ hiệu quả an ninh mạng của tổ chức.

# Kỹ thuật nhận dạng và ngăn chặn tấn công

## Những mối đe dọa từ không gian mạng

### Mối đe dọa không cấu trúc

công cụ tấn công và các script có rất nhiều trên internet, vì thế bất cứ ai tò mò đều có thể tài về và sử dụng chúng. Cũng có những người thích thú với việc xâm nhập vào mát tính và các hành động vượt qua khỏi tầm bảo vệ. Hầu hết tấn công không có cấu trúc đều được gây ra bởi Script Kiddies (những kẻ tấn công chỉ sử dụng các công cụ được cung cấp, không có hoặc có ít khả năng lập trình) hay những người có trình độ vừa phải. Hầu hết các cuộc tấn công đó vì sở thích cá nhân, nhưng cũng có nhiều cuộc tấn công có ý đồ xấu, những trường hợp đó ảnh hưởng xấu đến hệ thống cũng như hình ảnh của tổ chức bị tấn công.

Mặc dù tính chuyên môn của các cuộc tấn công dạng này không cao nhưng nó vẫn có thể phá hoại hoạt động của công ty và là một mối nguy hại lớn. Đôi khi chỉ cần chạy một đoạn mã là có thể phá hủy chức năng mạng của công ty. Một Script Kiddies có thể không nhận ra và sử dụng đoạn mã tấn công vào tất cả các host của hệ thống với mục đích truy cập vào mạng, nhưng kẻ tấn công đã vô tình gây ra sự gián đoạn cho cả một hệ thống. Hay trường hợp khác chỉ vì ai đó có ý định thử nghiệm khả năng, cho dù không có mục đích xấu nhưng cũng gây ra những tốn thất cho hệ thống

### Mối đe dọa có cấu trúc

Là các hành động cố ý, có động cơ và kỹ thuật cao, không như Script Kiddies, những kẻ tấn công này có đủ kỹ năng để hiểu các công cụ, có thể chỉnh sửa các công cụ hiện tại cũng như tạo ra các công cụ mới. Những kẻ tấn công này hoạt động độc lập hoặc theo nhóm. Họ hiểu, phát triển và sử dụng các kỹ thuật tấn công phức tạp nhằm thâm nhập vào mục tiêu.

Động cơ của các cuộc tấn công này thì có rất nhiều. Một số yếu tố thường thấy có thể vì tiền, hoạt động chính trị, sở hữu trí tuệ… Các tổ chức tội phạm, các đối thủ cạnh tranh hay các tổ chức sắc tộc có thể thuê các Hacker lành nghề để thực hiện các cuộc tấn công dạng này. Các cuộc tấn công thường có mục đích từ trước, cho dù động cơ là gì thì các cuộc tấn công như vậy đều gây ra hậu quả nghiêm trọng.

### Mối đe dọa từ bên ngoài

Là các cuộc tấn công được tạo ra khi không có một quyền hạn nào trong hệ thống, người dùng trên toàn thế giới thông qua internet đều có thể thực hiện các cuộc tấn công như vậy.

Các hệ thống bảo vệ vành đai là tuyến bảo vệ đầu tiên chống lại các cuộc tấn công dạng này. Bằng cách gia tăng hệ thống bảo vệ vành đai, ta có thể giảm tác động của kiểu tấn công này xuống tối thiểu. Mối đe dọa từ bên ngoài là mối đe dọa mà các công ty thường phải bỏ nhiều tiền và thời gian để ngăn ngừa

### Mối đe dọa từ bên trong

Thuật ngữ “mối đe dọa từ bên trong” được sử dugnj để mô tả một kiểu tấn công được thực hiện từ một người hoặc một tổ chức có một vài quyền truy cập mạng. Các cách tấn công từ bên trong được thực hiện từ một khu vực được tin cậy trong một hệ thống mang. Mối đe dọa này có thể khó phòng chống hơn vì các nhân viên có thể truy cập mạng và dữ liệu bí mật của công ty. Hầu hết các công ty chỉ có các tường lửa ở đường biên của mạng, và họ tin tưởng hoàn toàn vào các ACL (Access Control List) và quyền truy cập server để quy định cho sự bảo mật bên trong. Quyền truy cập server thường bảo vệ tài nguyên trên server nhưng không cung cấp bất kỳ sự bảo vệ nào cho mạng. Mối đe dọa từ bên trong thường được thực hiện bởi nhân viên bất mãn, muốn quay mặt với công ty. Nhiều phương pháp bảo mật liên quan đến vành đai của mạng, bảo vệ mạng bên trong khỏi các kế nối bên ngoài như là internet. Khi vành đai của mạng được bảo mật, các phần tin cậy bên trong có khuynh hướng bị giảm sự nghiêm ngặt. Khi một kẻ xâm nhập vượt qua vở bọc bảo mật đó. Những công việc còn lại rất đơn giản để dành quyền kiểm soát một hệ thống mạng.

## Kỹ thuật phát hiện và phòng chống xâm nhập

Có hai cách tiếp cận cơ bản đối với việc phát hiện và phòng chống xâm nhập là : phát hiện sự lạm dụng (Misuse Detection Model): Hệ thống sẽ phát hiện các xâm nhập bằng cách tìm kiếm các hành động tương ứng với các kĩ thuật xâm nhập đã được biết đến (dựa trên các dấu hiệu - signatures) hoặc các điểm dễ bị tấn công của hệ thống. phát hiện sự bất thường (Anomaly Detection Model): Hệ thống sẽ phát hiện các xâm nhập bằng cách tìm kiếm các hành động khác với hành vi thông thường của người dùng hay hệ thống.

### Phát hiện sự lạm dụng

Phát hiện sự lạm dụng là phát hiện những kẻ xâm nhập đang cố gắng đột nhập vào hệ thống mà sử dụng một số kỹ thuật đã biết. Nó liên quan đến việc mô tả đặc điểm các cách thức xâm nhập vào hệ thống đã được biết đến, mỗi cách thức này được mô tả như một mẫu. Hệ thống phát hiện sự lạm dụng chỉ thực hiện kiểm soát đối với các mẫu đã rõ ràng. Mẫu có thể là một xâu bit cố định (ví dụ như một virus đặc tả việc chèn xâu),…dùng để mô tả một tập hay một chuỗi các hành động đáng nghi ngờ.

Ở đây, ta sử dụng thuật ngữ kịch bản xâm nhập (intrusion scenario). Một hệ thống phát hiện sự lạm dụng điển hình sẽ liên tục so sánh hành động của hệ thống hiện tại với một tập các kịch bản xâm nhập để cố gắng dò ra kịch bản đang được tiến hành. Hệ thống này có thể xem xét hành động hiện tại của hệ thống được bảo vệ trong thời gian thực hoặc có thể là các bản ghi kiểm tra được ghi lại bởi hệ điều hành.

Các kỹ thuật để phát hiện sự lạm dụng khác nhau ở cách thức mà chúng mô hình hoá các hành vi chỉ định một sự xâm nhập. Các hệ thống phát hiện sự lạm dụng thế hệ đầu tiên sử dụng các luật (rules) để mô tả những gì mà các nhà quản trị an ninh tìm kiếm trong hệ thống. Một lượng lớn tập luật được tích luỹ dẫn đến khó có thể hiểu và sửa đổi bởi vì chúng không được tạo thành từng nhóm một cách hợp lý trong một kịch bản xâm nhập.

Để giải quyết khó khăn này, các hệ thống thế hệ thứ hai đưa ra các biểu diễn kịch bản xen kẽ, bao gồm các tổ chức luật dựa trên mô hình và các biểu diễn về phép biến đổi trạng thái. Điều này sẽ mang tính hiệu quả hơn đối với người dùng hệ thống cần đến sự biểu diễn và hiểu rõ ràng về các kịch bản. Hệ thống phải thường xuyên duy trì và cập nhật để đương đầu với những kịch bản xâm nhập mới được phát hiện.

Do các kịch bản xâm nhập có thể được đặc tả một cách chính xác, các hệ thống phát hiện sự lạm dụng sẽ dựa theo đó để theo vết hành động xâm nhập. Trong một chuỗi hành động, hệ thống phát hiện có thể đoán trước được bước tiếp theo của hành động xâm nhập. Bộ dò tìm phân tích thông tin hệ thống để kiểm tra bước tiếp theo, và khi cần sẽ can thiệp để làm giảm bởi tác hại có thể.

### Phát hiện sự bất thường

Dựa trên việc định nghĩa và mô tả đặc điểm của các hành vi có thể chấp nhận của hệ thống để phân biệt chúng với các hành vi không mong muốn hoặc bất thường, tìm ra các thay đổi, các hành vi bất hợp pháp. Như vậy, bộ phát hiện sự không bình thường phải có khả năng phân biệt giữa những hiện tượng thông thường và hiện tượng bất thường. Ranh giới giữa dạng thức chấp nhận được và dạng thức bất thường của đoạn mã và dữ liệu lưu trữ được định nghĩa rõ ràng (chỉ cần một bit khác nhau), còn ranh giới giữa hành vi hợp lệ và hành vi bất thýờng thì khó xác định hơn. Phát hiện sự không bình thường được chia thành hai loại tĩnh và động

**Phát hiện tĩnh**

Dựa trên giả thiết ban đầu là phần hệ thống được kiểm soát phải luôn luôn không đổi. Ở đây, ta chỉ quan tâm đến phần mềm của vùng hệ thống đó (với giả sử là phần cứng không cần phải kiểm tra). Phần tĩnh của một hệ thống bao gồm 2 phần con: mã hệ thống và dữ liệu của phần hệ thống đó. Hai thông tin này đều được biểu diễn dưới dạng một xâu bit nhị phân hoặc một tập các xâu. Nếu biểu diễn này có sự sai khác so với dạng thức gốc thì hoặc có lỗi xảy ra hoặc một kẻ xâm nhập nào đó đã thay đổi nó.

Lúc này, bộ phát hiện tĩnh sẽ được thông báo để kiểm tra tính toàn vẹn dữ liệu. Cụ thể là: bộ phát hiện tĩnh đưa ra một hoặc một vài xâu bit cố định để định nghĩa trạng thái mong muốn của hệ thống. Các xâu này giúp ta thu được một biểu diễn về trạng thái đó, có thể ở dạng nén. Sau đó, nó so sánh biểu diễn trạng thái thu được với biểu diễn tương tự được tính toán dựa trên trạng thái hiện tại của cùng xâu bit cố định. Bất kỳ sự khác nhau nào đều là thể hiện lỗi như hỏng phần cứng hoặc có xâm nhập.

Biểu diễn trạng thái tĩnh có thể là các xâu bit thực tế được chọn để định nghĩa cho trạng thái hệ thống, tuy nhiên điều đó khá tốn kém về lưu trữ cũng như về các phép toán so sánh. Do vấn đề cần quan tâm là việc tìm ra được sự sai khác để cảnh báo xâm nhập chứ không phải chỉ ra sai khác ở đâu nên ta có thể sử dụng dạng biểu diễn được nén để giảm chi phí. Nó là giá trị tóm tắt tính được từ một xâu bit cơ sở. Phép tính toán này phải đảm bảo sao cho giá trị tính được từ các xâu bit cơ sở khác nhau là khác nhau. Có thể sử dụng các thuật toán checksums, message-digest (phân loại thông điệp), các hàm băm.

Một số bộ phát hiện xâm nhập kết hợp chặt chẽ với meta-data (dữ liệu mô tả các đối tượng dữ liệu) hoặc thông tin về cấu trúc của đối tượng được kiểm tra. Ví dụ, meta-data cho một log file bao gồm kích cỡ của nó. Nếu kích cỡ của log file tăng thì có thể là một dấu hiệu xâm nhập.

**Phát hiện động**

Trước hết ta đưa ra khái niệm hành vi của hệ thống (behavior). Hành vi của hệ thống được định nghĩa là một chuỗi các sự kiện phân biệt, ví dụ như rất nhiều hệ thống phát hiện xâm nhập sử dụng các bản ghi kiểm tra (audit record), sinh ra bởi hệ điều hành để định nghĩa các sự kiện liên quan, trong trường hợp này chỉ những hành vi mà kết quả của nó là việc tạo ra các bản ghi kiểm tra của hệ điều hành mới được xem xét.

Các sự kiện có thể xảy ra theo trật tự nghiêm ngặt hoặc không và thông tin phải được tích luỹ. Các ngưỡng được định nghĩa để phân biệt ranh giới giữa việc sử dụng tài nguyên hợp lý hay bất thường. Nếu không chắc chắn hành vi là bất thường hay không, hệ thống có thể dựa vào các tham số được thiết lập trong suốt quá trình khởi tạo liên quan đến hành vi. Ranh giới trong trường hợp này là không rõ ràng do đó có thể dẫn đến những cảnh báo sai.

Cách thức thông thường nhất để xác định ranh giới là sử dụng các phân loại thống kê và các độ lệch chuẩn. Khi một phân loại được thiết lập, ranh giới có thể được vạch ra nhờ sử dụng một số độ lệch chuẩn. Nếu hành vi nằm bên ngoài thì sẽ cảnh báo là có xâm nhập. Cụ thể là: các hệ thống phát hiện động thường tạo ra một profile (dữ liệu) cơ sở để mô tả đặc điểm các hành vi bình thường, chấp nhận được. Một dữ liệu bao gồm tập các đo lường được xem xét về hành vi, mỗi đại lượng đo lường gồm nhiều chiều:

• Liên quan đến các lựa chọn: thời gian đăng nhập, vị trí đăng nhập,…

• Các tài nguyên được sử dụng trong cả quá trình hoặc trên một đơn vị thời gian: chiều dài phiên giao dịch, số các thông điệp gửi ra mạng trong một đơn vị thời gian,…

• Chuỗi biểu diễn các hành động.

Sau khi khởi tạo dữ liệu cơ sở, quá trình phát hiện xâm nhập có thể được bắt đầu. Phát hiện động lúc này cũng giống như phát hiện tĩnh ở đó chúng kiểm soát hành vi bằng cách so sánh mô tả đặc điểm hiện tại về hành vi với mô tả ban đầu của hành vi được mong đợi (chính là dữ liệu cơ sở), để tìm ra sự khác nhau. Khi hệ thống phát hiện xâm nhập thực hiện, nó xem xét các sự kiện liên quan đến thực thể hoặc các hành động là thuộc tính của thực thể. Chúng xây dựng thêm một dữ liệu hiện tại. Các hệ thống phát hiện xâm nhập thế hệ trước phải phụ thuộc vào các bản ghi kiểm tra (audit record) để bắt giữ các sự kiện hoặc các hành động liên quan. Các hệ thống sau này thì ghi lại một cơ sở dữ liệu đặc tả cho phát hiện xâm nhập. Một số hệ thống hoạt động với thời gian thực, hoặc gần thời gian thực, quan sát trực tiếp sự kiện trong khi chúng xảy ra hơn là đợi hệ điều hành tạo ra bản ghi mô tả sự kiện.

Khó khăn chính đối với các hệ thống phát hiện động là chúng phải xây dựng các dữ liệu cơ sở một cách chính xác, và sau đó nhận dạng hành vi sai trái nhờ các dữ liệu. Các dữ liệu cơ sở có thể xây dựng nhờ việc giả chạy hệ thống hoặc quan sát hành vi người dùng thông thường qua một thời gian dài.

## Sử dụng công nghê, kỹ thuật ngăn chặn tấn công

Có rất nhiều các giải pháp về kỹ thuật có thể áp dụng để phòng chống tấn công vào hệ thống máy tính. Các giải pháp phổ biến hiện nay là sử dụng tường lửa, hệ thống phát hiện và ngăn chặn xâm nhập, phòng chống mã độc hại, sử dụng các biện pháp mã hóa, …. Dưới đây chúng ta sẽ tìm hiểu cụ thể về các giải pháp này.

### Tường lửa

Tường lửa là một cơ chế để ngăn cách bảo vệ mạng tin cậy (trusted network) khỏi các mạng không tin cậy (untrusted network). Tường lửa như một trạm kiểm soát ở các điểm nối giữa các vùng, làm nhiệm vụ kiểm tra và quyết định luồng dữ liệu mạng có được đi qua hay không .

Tường lửa thường là trạm kiểm soát đầu tiên tiếp nhận luồng dữ liệu từ Internet để thực hiện xác định cho phép hay không cho phép một gói tin được đi vào hoặc đi ra. Giống như một nhân viên an ninh, đứng ở cửa tòa nhà, xác định cho phép hay không việc đi vào và đi ra tòa nhà đó. Nhờ đó, tường lửa giúp hạn chế khá nhiều các thông tin không được phép đi vào hệ thống mạng, gây ảnh hưởng tới hệ thống và ngăn chặn được nhiều các tấn công xâm nhập hệ thống, đặc biệt là tấn công từ chối dịch vụ.

Một tường lửa có thể hoạt động trên nhiều lớp khác nhau của mạng, từ lớp cao nhất là lớp ứng dụng cho đến lớp datalink (địa chỉ MAC). Phần lớn các tường lửa hoạt động trên lớp mạng và lớp giao giao vận. Chúng kiểm tra gói tin TCP/IP, sau đó ra quyết định dựa trên các thông tin trong gói tin đó như địa chỉ nguồn, địa chỉ đích, cổng nguồn, công đích hoặc tổ hợp của hai hay nhiều thông tin trên. Các tường lửa hoạt động trên lớp ứng dụng có thể kiểm soát theo nội dung, theo các từ khoá hoặc kiểm tra virus. Các tường lửa có nhiều loại khác nhau (hoạt động trên lớp mạng, lớp ứng dụng,…) nhưng chúng đều có chung đặc điểm trong nguyên tắc hoạt động: Tóm bắt dữ liệu, kiểm tra rồi quyết định cho đi qua, thay đổi thông tin (chỉnh sửa lại thông tin header,…) hay cấm. Một số tường lửa phức tạp hơn còn có khả năng yêu cầu xác thực (dưới dạng tên và mật khẩu hoặc theo dạng xác thực thẻ) trước khi cho phép truy cập. Tính năng này tương đối quan trọng vì việc kiểm soát theo địa chỉ IP trong nhiều trường hợp không đủ chặt chẽ. Người dùng dễ dàng đổi địa chỉ IP máy sang địa chỉ IP “tin cậy” và có đầy đủ các quyền truy cập của IP “tin cậy” này.

Tường lửa được chia làm 2 loại: tường lửa cứng và tường lửa mềm. Tường lửa cứng là loại tường lửa đi kèm theo một thiết bị phần cứng, thường được đặt tại ranh giới các vùng mạng để kiểm soát các thông tin đi qua mạng, hay còn gọi là tường lửa mạng. Tường lửa mềm là một chương trình phần mềm, được cài đặt trên một hệ thống phần cứng. Tường lửa cá nhân là một trong các loại tường lửa mềm.

Xét về công nghệ, thông thường hiện nay tường lửa được chia làm 3 công nghệ chính:

* Tường lửa lọc gói tin (Packet filter Firewall)
* Tường lức ứng dụng (Application level Gateway hay Proxy server)
* Tường lửa kiểm soát trạng thái (Stateful Inspection Firewall)

Tường lửa hoạt động dựa trên việc kiểm tra các gói tin thông qua bảng tập luật. Các luật được kiểm tra theo thứ tự từ trên xuống. Khi một gói tin phù hợp với một luật trong bảng tập luật, gói tin sẽ được xử lý theo các hành động được quy định: đi qua hoặc bị chặn lại tại tường lửa. Nếu trong bảng tập luật có các luật trùng nhau khi xử lý cùng một gói tin, thì luật ở trên sẽ được áp dụng và các luật phía dưới sẽ bị bỏ qua. Thông thường luật mặc định cuối cùng của tường lửa là từ chối tất cả các gói tin đi qua.

Tường lửa là trạm kiểm soát đầu tiên, do vậy cũng là nơi hứng chịu nhiều các nguy hại đến từ những kẻ tấn công có ý định xâm nhập vào hệ thống. Chính vì thế, để có thể kiểm soát tốt các kết nối vào ra, và tránh được các tấn công ảnh hưởng đến tường lửa thì việc đầu tiên là cần bảo vệ an toàn cho chính tường lửa. Các nguy hại không chỉ xảy đến từ bên ngoài mạng, mà chính những kết nối từ bên trong vùng được bảo vệ cũng có thể ảnh hưởng tới tường lửa. Giám sát các kết nối từ bên trong cũng như bên ngoài là hết sức cần thiết giúp bảo vệ tường lửa một cách chặt chẽ nhất. Ngoài ra, tường lửa được cấu hình đúng cũng lưu lại các hoạt động trong mạng. Những bản ghi này có thể là bằng chứng có giá trị trong việc truy tố những người tấn công bất hợp pháp vào hệ thống của chúng ta.

### Hệ thống IDS/IPS

Giải pháp thứ 2 để phòng chống tội phạm máy tính chính là hệ thống phát hiện và ngăn chặn xâm nhập IDS/IPS.

Phát hiện xâm nhập (Intrusion Detection) là quá trình giám sát các sự kiện xảy ra trong một hệ thống máy tính hoặc mạng và phân tích chúng để tìm ra các dấu hiệu của những rắc rối tiềm ẩn. Các dấu hiệu này được định nghĩa là sự vi phạm hoặc cố tình vượt qua các chính sách an ninh của máy tính, mạng. Các dấu hiệu xâm nhập có thể bị gây ra bởi nhiều nguyên nhân như sâu mạng, phần mềm gián điệp, kẻ tấn công đang cố gắng chiếm đoạt quyền truy cập hợp pháp vào máy tính từ Internet, người sử dụng hợp lệ có các hành vi vượt qua các đặc quyền truy cập được định trước hoặc lạm dụng đặc quyền của họ.

Phòng chống xâm nhập (Intrusion Prevention) là hành vi của hệ thống tự động ngăn chặn các xâm nhập trái phép, có khả năng gây hại cho hệ thống.

Một hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS) là phần mềm hoặc thiết bị chuyên dụng làm nhiệm vụ tự động thực hiện các hành động phát hiện xâm nhập.

Một hệ thống ngăn chặn xâm nhập (Intrusion Prevention System - IPS) là phần mềm hoặc một thiết bị chuyên dụng có khả năng phát hiện xâm nhập và có thể ngăn chặn các nguy cơ gây mất an ninh.

Các dấu hiệu của hành vi xâm nhập trái phép được định nghĩa là việc thực hiện các hành động bất hợp pháp hoặc vượt qua những cơ chế bảo mật của máy tính hay của mạng. Các vụ xâm nhập có thể là do kẻ tấn công truy cập vào hệ thống từ Internet, do những người dùng hợp pháp của hệ thống muốn đạt được sự truy cập vào các đặc quyền mà họ không đuợc phép, và do những người dùng hợp pháp lạm dụng đặc quyền của họ. Các hệ thống phát hiện xâm nhập là các sản phẩm phần cứng hoặc phần mềm trợ giúp quá trình giám sát và phân tích xâm nhập.

Nhiệm vụ chính của các hệ thông phát hiện và ngăn chặn xâm nhập là phòng chống cho một hệ thống máy tính bằng cách phát hiện các dấu hiệu tấn công và có thể đẩy lùi nó. Việc phát hiện các tấn công phụ thuộc vào số lượng và kiểu hành động thích hợp. Để ngăn chặn xâm nhập tốt cần phải kết hợp tốt giữa “bả và bẫy” được trang bị cho việc nghiên cứu các mối đe dọa. Việc làm lệnh hướng sự tập trung của kẻ xâm nhập vào tài nguyên được bảo vệ là một nhiệm vụ quan trọng khác. Cả hệ thống thực và hệ thống bẫy cần phải được kiểm tra một cách liên tục. Dữ liệu được tạo ra bằng các hệ thống phát hiện xâm nhập được kiểm tra một cách cẩn thận (đây là nhiệm vụ chính cho mỗi IDS) để phát hiện các dấu hiệu tấn công.

Hệ thống phát hiện xâm nhập là những chương trình hay thiết bị thực hiện việc tìm kiếm dấu hiệu của một xâm nhập bất hợp pháp. Ví dụ, một IDS/IPS có thể nhận thấy rằng một máy quét cổng đang xảy ra hoặc cho rằng ai đó đang cố gắng để đăng nhập vào với việc sử dụng tấn công SQL Injection. Hệ thống phát hiện xâm nhập sau đó có thể cảnh báo người quản trị về các hành vi truy cập vi phạm an ninh hệ thống và lưu lại chi tiết của các sự kiện như địa chỉ IP nguồn. Điều này có thể không chỉ cho phép chúng ta ngăn chặn các cuộc tấn công, mà còn cũng cung cấp bằng chứng để truy tố sau.

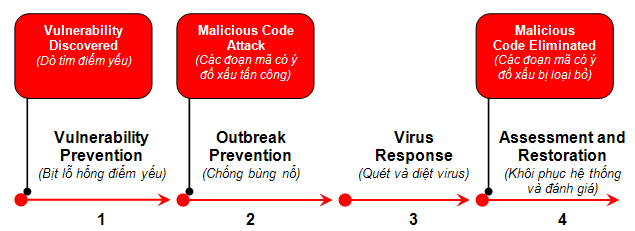
Có rất nhiều loại hệ thống phát hiện và ngăn chặn xâm nhập khác nhau, mỗi hệ thống có mức độ khác nhau về hiệu quả. Tuy nhiên không thể phủ nhận việc trang bị hệ thống IDS/IPS sẽ giúp tăng cường, cải thiện an ninh và chống được đáng kể các tấn công không đáng có ảnh hưởng tới hệ thống mạng. Ngoài ra, các bản ghi của một IDS/IPS, giống như các bản ghi tường lửa, có thể cung cấp bằng chứng có giá trị trong việc điều tra và truy tố bất kỳ tội phạm máy tính nào.

### Ngăn chặn mã độc hại

Internet là nơi vô cùng hữu ích cho mọi người truy xuất thông tin, hoặc thực hiện các giao dịch điện tử giữa các vùng cách xa nhau về địa lý. Tuy nhiên Internet lại là nơi mà các tội phạm và tin tặc trực tuyến luôn rình rập để gây rắc rối, đánh cắp các thông tin nhạy cảm của chúng ta. Một cách mà các tội phạm thường sử dụng đó là lây nhiễm và phát tán phần mềm độc hại. Chính vì thế, một giải pháp nữa cần được áp dụng để phòng chống tội phạm máy tính là ngăn chặn mã độc hại, ngăn chặn các nguy cơ lây lan của mã độc.

Mã độc hại được định nghĩa là “một chương trình được chèn một cách bí mật vào hệ thống với mục đích làm tổn hại đến tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của hệ thống”. Định nghĩa này sẽ bao hàm rất nhiều thể loại mà chúng ta vẫn quen gọi chung là virus máy tính ở Việt nam như: worm, trojan, spy-ware, ... thậm chí là virus hoặc các bộ công cụ để tấn công hệ thống mà các hacker thường sử dụng như: backdoor, rootkit, key-logger, ...

Để thực hiện ngăn chặn mã độc hại, cần phải thực hiện theo 4 giai đoạn như sau:



Hình 5.1. Mô hình phòng chống mã độc hại

* Giai đoạn 1: Là giai đoạn phòng vệ trên các lỗ hổng, điểm yếu của hệ thống mà virus cũng như các đoạn mã chương trình có ý đồ xấu có thể lợi dụng để tấn công vào hệ thống.
* Giai đoạn 2: Là giai đoạn phòng và chống virus bùng nổ trong hệ thống
* Giai đoạn 3: Là giai đoạn quét và diệt virus đã lây nhiễm trong hệ thống
* Giai đoạn 4: Là giai đoạn khôi phục sửa chữa những phần hệ thống đã bị virus làm hỏng. Khôi phục lại cho hệ thống hoạt động trở lại bình thường. Và đánh giá về mức độ thiết hại cũng như đánh giá rút ra kinh nghiệm về việc phòng chống virus vừa qua

Muốn bịt được lỗ hổng, điểm yếu của hệ thống thì cần phải có công cụ để kiểm soát, tìm xem trong hệ thống có những lỗ hổng điểm yếu nào đang tồn tại, phân loại các lỗ hổng điểm yếu nào là rất nguy hiểm có nguy cơ bị lợi dụng tấn công rất cao, loại nào bình thường, loại nào nguy cơ thấp. Cần phải có hệ thống cập nhật tập trung các miếng vá của Microsoft. Ngoài ra cần có công cụ để kiểm tra duy trì việc thực hiện các công việc trên, nói rộng ra là cần có công cụ để giám sát việc thực hiện việc thực hiện chính sách phòng chống mã độc hại.

Các mã độc hại thế hệ mới có tốc độ lây lan rất nhanh chỉ cần không đầy một giờ đồng hồ đã có thể lây lan, tràn ngập (hay còn gọi là bùng nổ) trong 1 mạng LAN, gây nghẽn, tê liệt hệ thống mạng và máy tính. Mã độc hại vẫn có thể gây bùng nổ với xác suất rất cao nếu hệ thống mạng đã có trang bị hệ thống phòng chống mã độc hại nhưng không có công cụ để phòng chống virus bùng nổ. Vì các sản phẩm phòng chống mã độc hại thông thường đều nhận dạng và diệt theo mẫu (được hãng cung cấp sản phẩm phát hành, và các khách hàng phải cập nhật cho hệ thống của mình) nhưng thời gian để các hãng cung cấp sản phẩm tìm ra và phát hành được mẫu mã độc hại thường không kịp để ngăn chặn virus bùng nổ. Vì thế hệ thống phòng chống mã độc hại cần được trang bị các công cụ nhằm ngăn chặn bùng nổ nhằm triển khai đồng loạt các chính sách chống bùng nổ xuống từng end-points.

Tiếp theo, hệ thống cần được trang bị các giải pháp đồng bộ nhằm ngăn chặn tất cả các con đường lây nhiễm và phát tán mã độc hại:

* Để ngăn chặn các tấn công ở lớp mạng (network service worm), cần có thiết bị chuyên dụng có khả năng dò quét, phát hiện và ngăn chặn các tấn công.
* Cần có giải pháp bảo vệ tại cổng kết nối internet nhằm ngăn chặn mã độc hại ngay tại gateway(kiểm soát các giao thức kết nối internet như: HTTP, HTTPS, SMTP, POP3)
* Cần có giải pháp ngăn chặn mã độc hại phát tán qua email
* Giải pháp ngăn chặn mã độc hại trên các end-point

Cuối cùng, giải pháp bảo vệ end-points cần có chức năng có khả năng làm sạch các rác do worm, trojant, spyware để lại trong hệ thống, giúp khôi phục sửa chữa các file hệ thống và registry của hệ thống đã bị virus làm hỏng.

Để thực hiện được 4 giai đoạn phòng chống mã độc hại như trên, ngoài các sản phẩm thì còn có một phần không thể thiếu và giữ vai trò rất quan trọng trong giải pháp phòng chống mã độc toàn diện đó là các dịch vụ hỗ trợ kỹ thuật. Các dịch vụ hỗ trợ kỹ thuật sẽ cung cấp cho khách hàng các kinh nghiệm, kỹ thuật của các chuyên gia phòng chống mã độc hại. Giúp cho khách hàng các thông tin nhanh, chính xác để đối phó với các mã độc hại nguy hiểm. Giúp khách hàng kiểm tra đánh giá tình trạng hoạt động của hệ thống phòng chống mã độc hại, đồng thời có các tư vấn hỗ trợ kỹ thuật để nâng cao hiệu quả hoạt động của hệ thống phòng chống mã độc hại, cũng như tư vấn về kế hoạch mở rộng, nâng cấp cho hệ thống phòng chống mã độc hại. Các chuyên gia cũng hỗ trợ kỹ thuật trong việc xử lý các sự cố khi vận hành hệ thống phòng chống mã độc hại giúp nâng cao tính sẵn sàng của hệ thống phòng chống mã độc hại và góp phần nâng cao tính sẵn sàng của hệ thống chung.

Ngoài ra giải pháp bảo mật cùng với chính sách bảo mật chung cho cả hệ thống cũng ảnh hưởng đến hiệu quả của hệ thống phòng chống mã độc hại. Cần phải kết hợp với các giải pháp bảo mật mạng khác để nâng cao tính an toàn cho hệ thống như FireWall (để kiểm soát truy nhập), xác thực mạnh (để chống việc giả mạo, mạo danh), Hệ thống phát hiện/phòng chống xâm nhập,… Vì chương trình, hệ thống diệt mã độc hại không thể đảm nhận được chức năng của các giải pháp khác mà kỹ thuật tấn công của mã độc hại ngày nay lại là sự kết hợp pha tạp rất nhiều kỹ thuật tấn công với nhau.

### Mã hóa

Một phương pháp nữa giúp phòng chống tội phạm máy tính là mã hóa. Mã hoá nhằm đảm bảo tính trong suốt của thông tin và ngăn chặn những kẻ tấn công bất hợp pháp xem, sửa đổi dữ liệu; bởi vì một khi thông tin đã được mã hoá và gửi đi thì kẻ xấu rất khó hoặc không thể giải mã được

Có 2 phương pháp mã hóa được sử dụng hiện nay là mã hóa đối xứng và mã hóa bất đối xứng. Hai loại mã hóa này khác nhau ở số lượng khóa. Mã hóa đối xứng sử dụng cùng một khóa để mã hóa/giải mã. Trong khi đó, mã hóa bất đối xứng sử dụng hai khóa khác nhau để mã hóa và giải mã thông tin. Mỗi hệ thống mã hóa có ưu nhược điểm riêng. Mã hóa đối xứng xử lí nhanh nhưng độ an toàn không cao. Mã hóa bất đối xứng xử lí chậm hơn, nhưng độ an toàn và tính thuân tiện trong quản lí khóa cao. Trong các ứng dụng mã hóa hiện tại, người ta thường kết hợp các ưu điểm của cả hai loại mã hóa này.

Mã hóa có vai trò rất quan trọng, đặc biệt là trong giao dịch điện tử. Nó giúp đảm bảo bí mật, toàn vẹn của thông tin, khi thông tin đó được truyền trên mạng. Mã hóa cũng là nền tảng của kĩ thuật chữ ký điện tử, hệ thống PKI...

Với những ưu điểm của mã hóa đem lại sẽ giúp cho chúng ta giảm thiểu nguy cơ do tội phạm máy tính đem lại.

### Các kỹ thuật, công nghệ khác

Ngoài các kỹ thuật, công nghệ đã nói ở trên; còn rất nhiều các giải pháp kỹ thuật khác cần được áp dụng để phòng chống tội phạm máy tính như:

* Sử dụng các giải pháp xác thực mạnh
* Sử dụng mạng riêng ảo
* Dò quét, đánh giá điểm yếu
* Chống tấn công mạng không dây
* ….

Tùy vào mục đích cũng như yêu cầu của hệ thống mà lựa chọn các giải pháp kỹ thuật phù hợp. Dĩ nhiên càng sử dụng nhiều giải pháp thì thông tin càng được bảo mật, song đi đôi với đó là chi phí trả cho việc bảo mật cũng tăng cao. Ngoài ra, hiệu năng cũng trái ngược với tốc độ. Càng sử dụng nhiều giải pháp bảo mật, có nghĩa là một gói tin muốn đi vào được hệ thống bên trong sẽ qua nhiều khâu kiểm tra; như vậy sẽ làm chậm băng thông của hệ thống. Chính vì thế cần cân đối các yếu tố để vừa có thể đảm bảo an toàn cho thông tin, tránh sự xâm nhập từ các tội phạm máy tính, trong khi đó vẫn đảm bảo được nhu cầu chi phí và đảm bảo hiệu suất hoạt động của toàn bộ hệ thống mạng.

# Những vấn đề an toàn thông tin trong hệ điều hành

## Các nguyên tắc cơ bản cho an toàn hệ thống thông tin

Khi đưa ra các vấn đề an toàn cho các máy chủ chúng ta không thể bỏ qua các nguyên tắc cơ bản cho sự an toàn thông tin nói chung:

* Sự đơn giản: Các lược đồ an toàn càng đơn giản, càng dễ thực hiện càng tốt.
* Dự phòng để đảm bảo an toàn: Nếu có sự cố sảy ra, hệ thống phải được đặt trong trạng thái mất an toàn (khi đó có thể một số chức năng của hệ thống sẽ bị cấm hoạt động). Chúng ta có thể để mất một số chức năng của hệ thống nhưng không để hệ thống mất an toàn.
* Sự điều chỉnh: Thay vì cho phép truy nhập trực tiếp đến các nguồn tài nguyên thông tin, các bộ điều khiển chính sách truy nhập được triển khai. Ví dụ, có thể sử dụng các quyền đối với hệ thống file, uỷ quyền, bức tường lửa, mail gateway.
* Thiết kế mang tính mở: Hệ thống an toàn không nên phụ thuộc vào sự bí mật của trong cài đặt hoặc phụ thuộc vào chính các thành phần của nó.
* Tách đặc quyền: Càng phân nhỏ được các chức năng càng tốt. Thuật ngữ phân tách chức năng có thể được áp dụng cho cả các hệ thống và cho cả các đối tượng sử dụng đầu cuối. Đối với các hệ thống, các chức năng như đọc, ghi, sửa, và thực thi cần được tách riêng. Tương tự như vậy, đối với người sử dụng đầu cuối các vai trò của họ cũng cần được tách riêng đến mức có thể.
* Đặc quyền tối thiểu: Việc thực hiện một chức năng không được gián tiếp hay trực tiếp ảnh hưởng đến chức năng khác.
* Tự nguyện: Người sử dụng nên hiểu sự cần thiết của vấn đề an toàn. Để đạt được điều đó có thể thông qua việc đào tạo và giáo dục người sử dụng. Bên cạnh đó, các lược đồ an toàn cần được xây dựng trên cơ sở góp ý của người dùng. Ví dụ, nếu người sử dụng nhận thấy các lược đồ an toàn là quá cồng kềnh, phức tạp trong các thao tác thực hiện, họ có thể cho những lời khuyên, như vậy tính thực tế của các lược đồ an toàn sẽ cao hơn.
* Cơ chế chung tối thiểu: Khi cung cấp khả năng truy nhập cho tiến trình máy chủ thư truy nhập đến một cơ sở dữ liệu thì không nên cấp quyền truy nhập đến cơ sở dữ liệu đó cho bất kỳ một ứng dụng nào khác trên hệ thống.
* Phòng bị có chiều sâu: cần hiểu rằng một lược đồ an toàn đơn sẽ không mang lại hiệu quả cao. Do đó, khi thiết kế các lược đồ an toàn cần tạo ra các tầng.
* Ghi lại các tấn công: Việc ghi lại nhật ký cần được duy trì, như vậy khi có sự cố chúng ta sẽ có các bằng chứng tấn công gây nên sự cố đó.

## Một số cơ chế bảo vệ tài nguyên ở mức hệ điều hành

Trong phần này, chúng ta xem xét một số cơ chế bảo vệ tài nguyên ở mức hệ điều hành, các cải tiến đối với cơ chế an toàn cơ bản dành cho hệ điều hành, thiết kế các hệ điều hành an toàn, tuỳ theo các chuẩn an toàn khác nhau.

Hệ điều hành thường được nhìn nhận là một hệ thống phân cấp trừu tượng của các chức năng, bắt đầu ở mức thấp nhất (mức phần cứng) của các kết nối vật lý và các thành phần điện tử, mức này cung cấp các chức năng nguyên thuỷ. Ở trên mức phần cứng là các mức trừu tượng khác của các chức năng hệ thống, tiếp đến là mức ứng dụng. Mỗi mức quản lý và kiểm soát tài nguyên của mình; Việc thực hiện các lệnh nguyên thuỷ của một mức được uỷ quyền cho các chương trình ở các mức thấp hơn. Mỗi mức được liên kết với một máy ảo (thao tác trên tài nguyên và thông qua ngôn ngữ của mức).

Kiến trúc điển hình của một hệ thống tính toán bao gồm các mức sau: phần cứng, cơ sở, hợp ngữ, hệ điều hành và một tập hợp các ứng dụng. Hệ điều hành đóng vai trò như là một giao diện giữa các chương trình ứng dụng và tài nguyên hệ thống.

OS (hệ điều hành) quản lý tất cả tài nguyên hệ thống (bộ nhớ, các file, thiết bị vào/ra, bộ xử lý) và tối ưu hoá việc sử dụng tài nguyên cho các chương trình ứng dụng khác nhau. Các chức năng của OS được tóm tắt như sau:

* Quản lý tiến trình và bộ xử lý (*process and processor management*): Chức năng này do nhân hệ điều hành cung cấp, nó hỗ trợ các tiến trình đồng thời của người dùng và hệ thống, với mục đích đảm bảo tối đa hiệu năng và tỷ lệ sử dụng tài nguyên của hệ thống.
* Quản lý tài nguyên (*resource management*): OS cấp phát tài nguyên hệ thống (như bộ nhớ, file, thiết bị vào/ra) cho các ứng dụng yêu cầu. OS giải quyết các xung đột có thể xảy ra giữa các chương trình dùng chung tài nguyên theo tiêu chí tối ưu hiệu năng và tốc độ xử lý của hệ thống.
* Giám sát (*supervision*): Với chức năng giám sát, OS tương tác trực tiếp với các chương trình ứng dụng, hỗ trợ việc thực hiện các ngôn ngữ ứng dụng khác nhau, lên lịch trình cho các tiến trình (tương ứng với các chương trình ứng dụng đang chạy). OS kiểm soát các chương trình đang chạy, không cho phép chúng sử dụng trái phép tài nguyên hệ thống, chống can thiệp gian lận hoặc ngẫu nhiên vào các vùng nhớ (được cấp phát trước cho các chương trình), hoặc giữa vùng nhớ dành cho các chương trình và vùng nhớ dành cho OS.

OS không ngừng phát triển, bắt đầu từ các chương trình đơn giản đến các hệ thống phức tạp, hỗ trợ các kiến trúc đa nhiệm vụ, đa xử lý, phân tán và xử lý thời gian thực. Tuỳ thuộc vào kiểu hệ thống, việc quản lý tài nguyên có thể đáp ứng được các mục đích và chính sách khác nhau.

Nói chung, OS cung cấp một số chức năng bảo vệ dữ liệu. Trong hệ thống xử lý, dữ liệu nằm trong một tài nguyên nào đó (ví dụ: bộ nhớ, file, thiết bị vào/ra); Với OS, việc bảo vệ dữ liệu có nghĩa là chỉ cho phép người dùng hợp pháp truy nhập vào tài nguyên (đối tượng) hệ thống.

Hình dưới đây minh hoạ các chức năng của một OS trong việc hỗ trợ an toàn, trong đó trình bày các giai đoạn cơ bản có trong một phiên làm việc của người dùng, trong một hệ thống đa người dùng. Hoạt động được bắt đầu bằng một yêu cầu kết nối với hệ thống (*giai đoạn đăng nhập*): OS nhận dạng người dùng thông qua các kỹ thuật nhận dạng và xác thực. Chỉ khi qua được giai đoạn này, người dùng mới có thể tiến hành các hoạt động, ví dụ làm việc trên các file (*quản lý hệ thống file*), hoặc chạy các chương trình (*thực hiện chương trình*). Việc chạy chương trình cần các vùng nhớ cấp phát trước. Chính vì vậy, nó phải được bảo vệ, tránh sự can thiệp của các chương trình khác và can thiệp từ bên ngoài (*bảo vệ bộ nhớ*). Một chương trình đang chạy có thể thực hiện các thao tác vào/ra (*quản lý vào/ra*).

Người dùng

Đăng nhập

Xác thực

Thực hiện chương trình

**Đăng xuất**

Quản lý hệ thống file

Bảo vệ bộ nhớ

Quản lý vào ra

Kiểm toán

Cấp phát tài nguyên

Kiểm soát truy nhập tài nguyên

Quản lý và phát hiện lỗi

Điều khiển luồng

Các chức năng dịch vụ của OS

**Các chức năng an toàn của OS**

*Hình 6.1: Phiên làm việc của người dùng*

OS hỗ trợ truy nhập đồng thời vào tài nguyên, chính vì vậy nó có thể giải quyết các xung đột có thể xảy ra (*cấp phát tài nguyên, kiểm soát truy nhập vào tài nguyên*). Các lỗi (xảy ra trong thời gian chạy) dẫn đến việc OS phải dừng chương trình nhằm hạn chế tối đa các thiệt hại có thể xảy ra đối với hệ thống, hoặc các chương trình khác (*phát hiện và quản lý lỗi*). Hơn nữa, OS còn lưu vết tất cả các thao tác mà người dùng đã thực hiện trên tài nguyên hệ thống, lưu các vết kiểm toán (*kiểm toán*). Cuối cùng, người dùng ngừng phiên làm việc và huỷ kết nối với hệ thống (*giai đoạn đăng xuất*).

Bên cạnh các chức năng dịch vụ (chẳng hạn như chạy chương trình, quản lý file, thao tác vào/ra, cấp phát tài nguyên, phát hiện và quản lý lỗi), các chức năng có thể hướng hỗ trợ an toàn là:

* Nhận dạng/xác thực người dùng
* Bảo vệ bộ nhớ
* Kiểm soát truy nhập vào tài nguyên
* Kiểm soát luồng
* Kiểm toán

## Kiểm soát truy cập

**Kiểm soát truy cập** (Access Control) chỉ ra khả năng của cơ quan/tổ chức trong việc kiểm soát sự truy cập vào các tài nguyên theo yêu cầu công việc và theo yêu cầu bảo mật, bao gồm:

* Có chính sách quản lý việc truy cập vào tài nguyên của cơ quan/tổ chức theo yêu cầu công việc và yêu cầu thông tin của từng cá nhân
* Có cơ chế để:
  + Đăng ký hoặc loại bỏ user
  + Kiểm tra kiểm soát quá trình truy cập và quyền hạn truy cập
  + Quản trị mật khẩu
* Thiết lập chính sách và cơ chế thích hợp để kiểm soát truy cập mạng, bao gồm:
  + Xác thực ở các điểm truy cập
  + Xác thực cho những người dùng bên ngoài cơ quan/tổ chức
  + Định nghĩa rõ ràng về chính sách định tuyến
  + Kiểm soát việc bảo vệ thiết bị mạng
  + Duy trì việc phân tách mạng thành các vùng khác nhau
  + Kiểm soát việc kết nối và truy cập mạng
  + Duy trì chế độ an toàn an ninh cho các dịch vụ mạng
* Thiết lập cơ chế kiểm soát truy cập vào máy chủ nhằm:
  + Tự động nhận diện kết nối từ trạm làm việc
  + Bảo mật khi đăng cập
  + Xác thực người sử dụng
  + Quản lý mật khẩu đăng cập
  + Bảo vệ các tài nguyên hệ thống
  + Giới hạn khả năng thao tác của user
* Có chính sách để giới hạn quyền truy cập ứng dụng dựa trên quyền hạn và mức độ phân quyền của người sử dụng
* Có cơ chế để theo dõi các hành động truy cập hệ thống và phát hiện các truy cập bất hợp pháp
* Thiết lập chính sách và tiêu chuẩn chỉ ra việc bảo vệ tài nguyên, bảo mật truy cập và trách nhiệm của những người sử dụng kết nối từ bên ngoài hệ thống

## Nhận dạng/xác thực người dùng

Các hệ thống xác thực dựa vào thông tin người dùng biết (*information known to the user*) là:

* Các hệ thống dựa vào mật khẩu (*password-based systems*): Người dùng được nhận dạng, thông qua một chuỗi ký tự bí mật (mật khẩu), chỉ có người dùng và hệ thống biết.
* Các hệ thống dựa vào hỏi đáp (*query-answer-based systems*): Người dùng được nhận dạng, thông qua việc trả lời một tập hợp các câu hỏi mà hệ thống đặt ra. Các câu hỏi được đặt riêng cho từng người và chủ yếu dựa vào các hàm toán học (do hệ thống tính toán sau khi nhận được các giá trị đầu vào từ người dùng).
* Các hệ thống xác thực hai lần (*double authentication systems*): hệ thống tự giới thiệu mình với người dùng, còn người dùng tự xác thực ngược trở lại hệ thống. Xác thực hệ thống dựa vào các thông tin chỉ có người dùng biết (ví dụ, ngày, giờ và đoạn chương trình của phiên làm việc cuối). Xác thực người dùng dựa vào mật khẩu.

Về cơ bản, các hệ thống xác thực dựa vào thông tin người dùng sở hữu (*information owned by the user*) là các hệ thống dựa vào thẻ (*card-based systems*): thẻ từ có chứa một mã vạch, hoặc mã vạch từ, hoặc một bộ vi xử lý. Việc xác thực xảy ra tuỳ thuộc vào sự chấp nhận thẻ (được đưa vào trong thiết bị đọc), đôi khi được gắn kèm với một mã bí mật (*secret code*). Các hệ thống xác thực như sau:

* Các hệ thống nhận dạng qua ảnh (*computerized facsimile systems*): Ảnh của người dùng được lưu giữ; Việc nhận dạng được thực hiện bằng cách đối chiếu người này với ảnh được lưu giữ hiển thị trên màn hình;
* Các hệ thống nhận dạng qua dấu vân tay (*Fingerprint-based systems*): Việc nhận dạng được thực hiện bằng cách đối chiếu dấu vân tay của người dùng với dấu vân tay được lưu giữ;
* Các hệ thống nhận dạng qua đặc trưng của chữ ký viết bằng tay (*hand- pressure systems*): Việc nhận dạng được thực hiện dựa vào độ nhấn của tay người dùng khi ký trên một thiết bị thích hợp.
* Các hệ thống nhận dạng qua tiếng nói (*voice recognition-based systems*): So sánh giọng nói của người dùng với giọng nói được lưu giữ.
* Các hệ thống nhận dạng qua đặc điểm võng mạc (*retinal features- based systems*): Việc nhận dạng được thực hiện bằng cách kiểm tra các đặc điểm võng mạc của người dùng.

Các hệ thống xác thực này có độ phức tạp cao hơn so với các hệ thống xác thực đã được liệt kê trước, do sự phức tạp khi đối chiếu các đặc điểm được lưu giữ của cá nhân với con người thực tế. Do đó, xác xuất từ chối người dùng hợp pháp cao hơn. Tiếp theo là vấn đề chi phí, các kỹ thuật đi kèm (như nhận dạng tiếng nói/ảnh) làm nâng giá thành của hệ thống (rất đắt). Do vậy, việc sử dụng nó chỉ thích hợp trong các môi trường an toàn cao và thiết yếu.

Không phải tất cả các cơ chế nêu trên đều được thực hiện tại mức OS, cơ chế xác thực dựa vào mật khẩu được sử dụng phổ biến nhất. Chúng ta sẽ đi sâu xem xét các cơ chế này.

**Xác thực dựa vào mật khẩu**

Mật khẩu là một chuỗi ký tự bí mật (số hoặc chữ), chỉ có người dùng và hệ thống biết, do đó hệ thống có khả năng nhận dạng duy nhất người dùng dựa vào việc xác nhận tính hợp lệ của mật khẩu (phê chuẩn). Những vấn đề trong việc sử dụng mật khẩu phụ thuộc vào sự lựa chọn ban đầu, khả năng khám phá mật khẩu cho các mục đích gian lận, quản lý mật khẩu.

Các tiêu chuẩn đối với mật khẩu 'bí mật' là:

* Sử dụng ít nhất 8 ký tự, nói chung nên sử dụng các mật khẩu dài;
* Sử dụng cả số và chữ;
* Sử dụng cả chữ thường và chữ in hoa;
* Sử dụng các ký hiệu bàn phím đặc biệt (ví dụ, &,@ và %);
* Chọn các từ nước ngoài;
* Sử dụng các chuỗi ký tự bàn phím, sao cho có thể lưu giữ dễ dàng (ví dụ, sử dụng 4 ký tự cuối của hàng 2; các chữ cái trong cột thứ 3 của bàn phím,v.v);

Người dùng nên:

* Chọn mật khẩu tuân theo tiêu chuẩn trên;
* Ghi nhớ mật khẩu của mình, không bao giờ được viết ra;
* Không bao giờ để lộ mật khẩu của mình;
* Thay đổi mật khẩu thường xuyên và định kỳ.

Một số hệ thống tự động huỷ bỏ mật khẩu khi thời hạn tồn tại của nó kết thúc, từ đó bắt buộc người dùng phải thay đổi mật khẩu định kỳ.

Nên tránh sử dụng luân phiên cùng mật khẩu, một số hệ thống tự động kiểm tra và phòng tránh điều này. Chỉ có người dùng hợp pháp và hệ thống biết mật khẩu; Chủ nhân của mật khẩu trao kết nối cho hệ thống và sử dụng tài nguyên của hệ thống này. Do vậy, không nên để xảy ra tình trạng khám phá mật khẩu.

Thông thường, mật khẩu phải được lưu giữ trong một hệ thống đa người dùng, nhằm đáp ứng các hoạt động xác thực sau này. Do vậy, mật khẩu phải được lưu giữ trong một file do OS quản lý, sao cho mỗi định danh người dùng gắn với một (nhiều) mật khẩu. Khi kiểm tra, tiến hành đối chiếu mật khẩu gõ vào và mật khẩu được lưu giữ.

Cũng có thể biết được mật khẩu hợp lệ thông qua file mật khẩu, vì vậy yêu cầu bảo vệ các file này rất lớn, mật khẩu được lưu giữ trong một vùng nhớ mà chỉ có OS mới có khả năng truy nhập vào đó, nhưng cũng có nghĩa là tất cả các modun của OS được phép truy nhập vào file này. Người dùng có thể lợi dụng các modun dễ bị tấn công của OS, truy nhập vào và biết được nội dung của file. Ngoài ra, chúng ta có thể sử dụng một số thủ tục truy nhập file mật khẩu (ví dụ, thủ tục đăng nhập), nhưng các cá nhân có thể đọc toàn bộ bộ nhớ và truy nhập vào vùng nhớ có chứa file này.

Các trở ngại này có thể được giải quyết trong một số hệ thống, bằng cách mã hoá mật khẩu (có sử dụng các thuật toán mã hoá). Sau khi được tạo ra, mật khẩu được mã hoá và lưu giữ trong các file mật khẩu, người dùng có thể đọc nó nhưng việc sửa đổi (chèn, xoá, cập nhật) do OS thực hiện. Việc bảo vệ phụ thuộc vào việc chọn lựa các thuật toán mã hoá, sao cho việc giải mã phức tạp và tốn kém, cả về thời gian và tính toán.

Với các biện pháp trên, rủi ro xâm nhập gian lận vẫn có thể xảy ra, cần kết hợp chúng với việc quản lý mật khẩu.

## Nhật ký hệ thống

Ghi nhật ký là một yếu tố quan trọng trong lĩnh vực an toàn nói chung. Việc ghi nhật ký chính xác và theo dõi thông tin được ghi trong nhật ký là rất cần thiết. Các tệp nhật ký thường chỉ ghi lại các sự kiện đáng ngờ. Cần thiết lập các cơ chế ghi lại các thông tin trên và sử dụng các thông tin đó để tạo cơ sở cho việc phát hiện sự xâm nhập trái phép.

Nhật ký mạng và hệ thống có thể cảnh báo người quản trị máy chủ khi có một sự kiện nghi ngờ xuất hiện. Kết hợp với việc phân tích các thông tin bổ sung từ nhật ký của chính phần mềm trên máy chủ, chúng ta có thể suy đoán được nguyên nhân, mục đích của sự kiện trên.

Một số chức năng của nhật ký phần mềm máy chủ:

* Cảnh báo cho các hoạt động bị nghi ngờ cần được điều tra thêm.
* Ghi lại dấu vết các hoạt động của đối tượng xâm nhập
* Hỗ trợ việc phục hồi hệ thống
* Hỗ trợ việc điều tra các sự kiện xuất hiện tiếp theo
* Cung cấp các thông tin cho việc xử lý tranh chấp

Việc lựa chọn và triển khai phần mềm máy chủ cụ thể sẽ quyết định việc thiết lập cấu hình ghi nhật ký cho các nhà quản trị.

*Thiết lập cấu hình ghi nhật ký*

Khả năng ghi nhật ký của các máy chủ là khác nhau, dưới đây chỉ đề cập đến các cấu hình chung nhất. Nên thiết lập chế độ ghi nhật ký 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 (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

Phần mềm máy chủ cung cấp khả năng cho phép hoặc vô hiệu hoá việc các điều khiển truy nhập xác định trong 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.

*Tổng kết và duy trì nhật ký*

Tổng kết các tệp nhật ký là một yêu cầu thực tế và nó có thể đòi hỏi mất nhiều thời gian. Các tệp nhật ký phản ánh mức độ an toàn của hệ thống, vì chức năng của chúng là ghi lại các sự kiện đã sảy ra. Ngoài ra, các tệp này thường rất có ích trong việc cung cấp các thông tin khác như việc sử dụng CPU, lưu lượng mạng bất thường. Khi các tệp nhật ký được sử dụng để chứng thực các bằng chứng khác, việc tổng kết lại nhật ký sẽ tuân theo thứ tự. Tần số việc tổng kết nhật ký phụ thuộc vào các yếu tố sau đây:

* Lưu lượng máy chủ nhận được
* Mức đe doạ chung.
* Các mối đe doạ xác định.
* Các lỗ hổng của máy chủ
* Giá trị dữ liệu và các dịch vụ được máy hỗ trợ

Các bản tổng kết này sẽ được thực hiện hàng ngày, hàng tuần hay khi một hành động đáng ngờ xuất hiện. Công việc này có thể trở thành gánh nặng cho người quản trị. Để giảm gánh nặng này cho các nhà quản trị, các công cụ phân tích tự động các tệp nhật ký đã được phát triển.

Tuy nhiên, việc phân tích các tệp nhật ký cần được thực hiện chi tiết hơn. Bởi vì một tấn công tiêu biểu có thể bao gồm hàng trăm yêu cầu được gửi tới máy chủ, trong khi đó kẻ tấn công có thể cố gắng che dấu sự tấn công của mình bằng cách tăng khoảng cách giữa hai lần gửi yêu cầu. Trong trường hợp này việc tổng kết nhật ký theo từng ngày riêng hoặc từng tuần có thể không nhận ra sự tấn công. Khi tăng thời gian tổng kết nhật ký kê theo tháng hoặc theo quí, nhiều tấn công xuất phát từ cùng một máy hoặc cùng một lớp mạng sẽ dễ dàng bị nhận ra.

Các tệp nhật ký cần được bảo vệ để đảm bảo rằng nếu kẻ tấn công thực hiện phá hoại một máy chủ, các tệp nhật ký sẽ không bị thay đổi nhằm che dấu cuộc tấn công đó. Mặc dù phương pháp mã hoá bảo vệ các tệp nhật ký, nhưng giải pháp tốt nhất là để lưu trữ các tệp nhật ký là nên ghi chúng lên một máy riêng (không cùng với máy chủ). Máy này thường được gọi là các máy nhật ký hay các máy nhật ký hệ thống.

Các tệp nhật ký nên được lưu dự phòng một cách thường xuyên. Việc lưu dự phòng các tệp nhật ký theo từng giai đoạn thời gian có thể rất quan trọng bởi nhiều lý do: làm bằng chứng pháp lý, các vấn đề đã sảy ra đối với chủ, ... Việc chia khoảng thời gian để lưu dự phòng các tệp nhật ký phụ thuộc vào các yếu tố::

* Các yêu cầu pháp lý
* Các yêu cầu của tổ chức
* Dung lượng nhật ký
* Giá trị của các dịch vụ và dữ liệu
* Mức đe doạ

*Các công cụ phân tích tự động tệp nhật ký*

Lưu lượng dữ liệu truyền qua máy chủ 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 nhằm làm giảm gánh nặng cho các nhà quản trị. Các dụng cụ này phân tích các tệp nhật ký trên máy chủ 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.

## Đánh giá khả năng an toàn của hệ điều hành

Nếu không thực hiện việc kiểm tra, sẽ không khẳng định được rằng các biện pháp an toàn hiện tại có thể hoạt động, các biện pháp lấp lỗ hổng được người quản trị áp dụng có thực hiện đúng các chức năng như đã quảng cáo hay không? Hiện tại có rất nhiều công nghệ kiểm tra sự an toàn, nhưng phương pháp quét lỗ hổng được biết đến như một phương pháp phổ thông nhất. Việc thực hiện quét lỗ hổng giúp người quản trị xác định các lỗ hổng và kiểm tra xem các biện pháp an toàn hiện đang được áp dụng có hiệu quả hay không. Việc kiểm tra sự thâm nhập trái phép cũng được sử dụng nhưng không thường xuyên và thường chỉ là một phần trong việc tổng kiểm tra thâm nhập trái phép cho mạng chung của cả tổ chức.

### 6.6.1 Quét lỗ hổng

Quét lỗ hổng là việc sử dụng các công cụ hoạt động tự động, nhằm xác định các lỗ hổng và cấu hình sai của máy chủ. Trong đó có nhiều sản phẩm quét lỗ hổng có cả chức năng cung cấp thông tin về việc làm giảm nhẹ thiệt hại do các lỗ hổng đã được phát hiện gây nên.

Các công cụ quét lỗ hổng cố gắng xác định các lỗ hổng trên các máy được quét. Các lỗ hổng có thể là: các phiên bản phần mềm quá hạn, lỗi lấp lỗ hổng, lỗi nâng cấp hệ thống, … cho các máy chủ. Để hoàn thành được các chức năng trên, các công cụ quét lỗ hổng trước hết thường xác định cụ thể hệ điều hành, các ứng dụng phần mềm chính hiện có trên máy chủ sau đó kiểm tra các lỗ hổng đã được phát hiện trước đây đối với chúng. Việc kiểm tra trên được thực hiện trên một cơ sở dữ liệu lớn lưu các lỗ hổng đã được phát hiện trên các hệ điều hành và các ứng dụng phổ thông, hay được sử dụng hiện nay.

Tuy nhiên, các công cụ quét lỗ hổng cũng có một số điểm yếu. Nhìn chung, các công cụ này chỉ định danh được lỗ hổng mà không đánh giá độ rủi ro chung cho máy chủ được quét. Mặc dù quá trình quét đã được tự động hoá, nhưng các công cụ quét lỗ hổng cũng thường có tỷ lệ lỗi khá cao (ví dụ một lỗi thường gặp trong các công cụ quét lỗ hổng là đưa ra các báo cáo đối với các lỗ hổng không tồn tại). Điều này có nghĩa là để có một kết quả chính xác các chuyên gia, người quản trị cần có một bước phân tích thêm. Hơn nữa, các công cụ quét lỗ hổng không có khả năng định danh cho các lỗ hổng cho các chương trình, các ứng dụng do người dùng xây dựng.

Các công cụ quét lỗ hổng phụ thuộc vào giai đoạn cập nhật cơ sở dữ liệu các lỗ hổng để nhận biết các lỗ hổng mới nhất. Trước khi chạy công cụ quét, người quản trị nên cài đặt sự cập nhật mới nhất cho các cơ sở dữ liệu lỗ hổng. Tần số của việc cập nhật cơ sở dữ liệu lỗ hổng phụ thuộc vào từng công cụ quét.

Các công cụ quét lỗ hổng thường hiệu quả trong việc phát hiện ra các lỗ hổng đã được biết đến nhiều hơn là các lỗ hổng ít xuất hiện vì không thể có một sản phẩm nào lại có thể định danh được tất cả các lỗ hổng đã biết trong một khoảng thời gian nhất định. Hơn nữa, các nhà xây dựng công cụ quét thường muốn công cụ của mình có thể chạy với tốc độ nhanh (muốn phát hiện nhiều lỗ hổng thì cần nhiều phép thử, như vậy sẽ làm chậm tiến trình quét chung).

Các công cụ quét lỗ hổng có thể cung cấp các khả năng sau:

* Định danh các máy đang hoạt động trên mạng
* Định danh các dịch vụ (cổng) hiện đang được kích hoạt trên các máy.
* Định danh các ứng dụng.
* Định danh các hệ điều hành.
* Định danh các lỗ hổng tương ứng với hệ điều hành và các ứng dụng đã phát hiện.
* Kiểm tra việc tuân thủ chính sách an toàn của các ứng dụng trên máy chủ.

Việc quét lỗ hổng cần sự trợ giúp từ sức lao động với trình độ cao của con người trong việc giải thích kết quả của quá trình quét. Nó cũng có thể gây tổn hại đến hoạt động của mạng do quá trình quét sẽ làm tăng băng thông và giảm thời gian đáp ứng trên mạng. Tuy nhiên, việc quét lỗ hổng là rất quan trọng cho việc làm giảm bớt các lỗ hổng, trước khi chúng bị phát hiện và được khai thác bởi các mục đích bất hợp pháp. Việc quét lỗ hổng nên được thực hiện theo định kỳ hàng tuần, hàng tháng, hoặc khi nào cơ sở dữ liệu lỗ hổng mới được phát hành.

Nói chung, trên thực tế nên sử dụng nhiều hơn một công cụ quét lỗ hổng, bởi như đã đề cập ở trên, không có một công cụ nào có thể phát hiện được tất cả các lỗ hổng đã được biết. Theo các chuyên gia trong lĩnh vực này, nên sử dụng hai công cụ quét lỗ hổng, một thuộc lớp các sản phẩm thương mại, một thuộc lớp các sản phẩm miễn phí.

Các kết quả của quá trình quét cần được đóng thành tài liệu phục vụ cho việc phân tích, đánh giá. Cần chú ý rằng đối với các công cụ quét không phải là các sản phẩm thương mại, thì kết quả của quá trình quét nhất định phải được chính xác hoá thông qua sự phân tích của các chuyên gia.

### 6.6.2. Tấn công thử

Tấn công thử là một phép kiểm tra sự an toàn, trong đó các nhà đánh giá độ an toàn cố gắng tấn công các tính năng an toàn của hệ thống trên cơ sở những hiểu biết của họ về thiết kế và qui trình triển khai hệ thống đó. Mục đích của việc tấn công thử nhằm đánh giá sức chịu của các biện pháp bảo vệ hệ thống, thông qua việc sử dụng các công cụ và kỹ thuật chung đã được các hacker phát triển. Tấn công thử là một yêu cầu không thể thiếu trong các hệ thống mạng quan trọng và phức tạp.

Việc tấn công thử có thể không có mấy ý nghĩa đối với chương trình an toàn thông tin của các tổ chức. Tuy nhiên, nó là công việc yêu cầu trình độ cao (ở mức chuyên gia) nhằm tối thiểu hoá rủi ro cho các hệ thống được sử dụng làm mục tiêu tấn công thử. Quá trình tấn công thử có thể làm cho mạng hoạt động chậm, thậm chí có bị thể phá huỷ.

Tấn công thử sẽ đem lại cho chúng ta các lợi ích sau đây:

* Kiểm tra mạng sử dụng các phương pháp và công cụ mà các hacker thường sử dụng để tấn công.
* Kiểm tra sự tồn tại của các lỗ hổng.
* Không chỉ dừng lại ở việc xác định lỗ hổng mà còn giải thích cho việc có thể khai thác các lỗ hổng này để tấn công.
* Chứng minh các lỗ hổng không chỉ tồn tại đơn thuần trên lý thuyết.
* Hỗ trợ về mặt phương pháp luận cho việc giải quyết các vấn đề an toàn.

## Cài đặt các bản “vá” hệ điều hành

Việc cài đặt các bản “vá” hệ điều hành giúp cho hệ thống máy chủ giảm thiểu và ngăn chặn các cuộc tấn công đã biết vì thế trong đảm bảo an toàn thông tin cho hệ điều hành thì:

* Các máy chủ cần đuợc cài đặt kịp thời và chính xác các bản vá hệ điều hành cũng như bản vá ứng dụng. Điều này ngăn chặn các tấn công nhằm khai thác các điểm yếu bảo mật để phá hoại hệ thống.
* Nên thường xuyên theo dõi thông tin công khai từ các nhà cung cấp sản phẩm hoặc thông tin cảnh báo về lỗ hổng bảo mật từ các nguồn tin cậy (cơ quan CERT của chính phủ, các trung tâm, công ty có uy tín về bảo mật) để nắm được cơ chế và mức độ nguy hại khi điểm yếu bảo mật bị lợi dụng.
* Việc theo dõi và áp dụng bản vá cũng cần có qui trình và thử nghiệm cẩn thận, theo từng bước một và có phương án dự phòng để khôi phục lại hệ thống như trước khi cài bản vá.
* Cần phải cảnh giác với các thông báo và các bản vá xuất phát từ những nguồn không tin cậy. Có thể việc chạy các bản vá giả mạo này sẽ gây nhiễm virus vào hệ thống (vì đây có thể là cách để hacker giepo rắc, phát tán virus) hoặc ngay lập tức phá huỷ hệ thống.
* Việc thực thi tải xuống và cài đặt bản vá có thể được thực hiện trực tiếp từ nhà cung cấp sản phẩm, thông qua đường Internet, hoặc thông qua hệ thống quản lý bản vá tập trung. ví dun như Microsoft cung cấp cả hai giải pháp, cập nhật từ website của Microsoft hoặc cập nhật từ hệ thống SUS hoặc WUS. Có một số hãng như PatchLink hoặc BigFix cũng cung cấp các giải pháp tự động quản lý bản vá cho tất cả các loại hệ điều hành và ứng dụng.

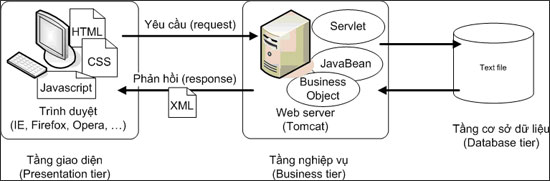
# Đảm bảo an toàn ứng dụng Web, máy chủ thư điện tử

## Kiến trúc hệ thống ứng dụng web, máy chủ thư điện tử

Một ứng dụng web khi triển khai, về cơ bản sẽ có ba lớp như sau: lớp trình diễn, lớp ứng dụng và lớp cơ sở dữ liệu. Việc nắm vững các mô hình triển khai của các hệ thống web sẽ giúp đỡ nhiều trong quá trình kiểm thử bảo mật hệ thống web cũng như việc tăng cường hệ thống bảo mật cho website của mình.

**Lớp trình diễn**

Lớp trình diễn hay còn gọi là máy chủ phục vụ web hoặc Web Server. Nó đơn giản là một máy chủ phục vụ được cài đặt các chương trình phục vụ cho web (ftp, www,…) và có thể xuất bản được những trang web ra ngoài Internet. Nó lắng nghe những yêu cầu từ phía người dùng (client), ví dụ như từ một trình duyệt và xử lý những yêu cầu đó, sau đó trả kết quả dưới dạng một form chứa các trang được định dạng dưới dạng văn bản hoặc hình ảnh. Trình duyệt sẽ hiển thị những kết quả này lên một cách tốt nhất đến client.



*Hình 7.1: Hoạt động của web server*

Một số máy chủ web server thông dụng hiện nay:

*Máy chủ IIS (Internet Information Services)*

Đây là một thành phần có sẵn trong các phiên bản của của hệ điều hành Microsoft Windows. Nó cung cấp, phát tán các thông tin lên mạng Internet và bao gồm nhiều dịch vụ khác nhau như Web Server, FTP Server,… Nó có thể được sử dụng để xuất bản nội dung của các trang Web lên Internet bằng việc sử dụng Hypertext Transport Protocol (HTTP). Máy chủ IIS có thể thực thi một số kiểu file chuyên biệt của ngôn ngữ ASP (\*.asp, \*.aspx, … ).

*Máy chủ Apache HTTP*

Apache là phần mềm web server nổi tiếng, đóng vai trò quan trọng trong sự phát triển ban đầu của World Wide Web. Apache được phát triển và duy trì bởi cộng đồng mã nguồn mở dưới sự bảo trợ của Apache Software Foundation với rất nhiều ứng dụng có sẵn cho nhiều hệ điều hành bao gồm cả Unix, GNU, FreeBSD, Linux, Solaris, Novell Netware, AmigaOS, Mac OS X, Microsoft Windows, … Apache hỗ trợ đa tính năng, người sử dụng có thể biên dịch thêm các module để mở rộng chức năng ngoài chức năng cốt lõi của Apache. Apache có thể thực thi các file chuyên biệt của ngôn ngữ PHP (\*.php).

*Máy chủ Apache Tomcat*

Apache Tomcat là một Java Servlet được phát triển bởi Apache Software Foundation (ASF). Tomcat thi hành các ứng dụng Java Servlet và JavaServer Pages (\*.jsp) từ Sun Microsystems và cung cấp một máy chủ HTTP cho ngôn ngữ Java thuần túy để thực thi các chương trình lệnh viết bằng ngôn ngữ Java.

*Các máy chủ phục vụ web khác*

Ngoài các máy chủ thường sử dụng trên thi còn một số máy chủ phục vụ web khác vẫn được sử dụng như: nginx, GWS, lighttpd, SunOne…

**Lớp ứng dụng**

Lớp ứng dụng hay Web Application, là nơi các kịch bản hay mã nguồn phát triển ra ứng dụng web được thực thi. Lớp này sẽ biên dịch các mã nguồn tương ứng và thực hiện các truy vấn đến cơ sở dữ liệu dựa vào mã nguồn ứng dụng.

Một số ngôn ngữ thực thi mã nguồn ứng dụng web:

*ASP.NET*

ASP.NET là một nền tảng ứng dụng web (web application framework) được phát triển và cung cấp bởi Microsoft, cho phép những người lập trình tạo ra những trang web động, những ứng dụng web và những dịch vụ web. Lần đầu tiên được đưa ra thị trường vào tháng 2 năm 2002 cùng với phiên bản 1.0 của .NET framework, là công nghệ nối tiếp của Microsoft Active Server Pages (ASP). ASP.NET được biên dịch dưới dạng Common Language Runtime (CLR), cho phép những người lập trình viết mã ASP.NET với bất kỳ ngôn ngữ nào được hỗ trợ bởi .NET language.

*PHP*

PHP (Hypertext Preprocessor) là một ngôn ngữ lập trình kịch bản hay một loại mã lệnh chủ yếu được dùng để phát triển các ứng dụng viết cho máy chủ, mã nguồn mở, dùng cho mục đích tổng quát. Nó rất thích hợp với web và có thể dễ dàng nhúng vào trang HTML. Do được tối ưu hóa cho các ứng dụng web, tốc độ nhanh, nhỏ gọn, cú pháp giống C và Java, dễ học và thời gian xây dựng sản phẩm tương đối ngắn hơn so với các ngôn ngữ khác nên PHP đã nhanh chóng trở thành một ngôn ngữ lập trình web phổ biến nhất thế giới.

*JSP*

JSP (JavaServer Pages) còn được biết đến với một cái tên khác là Java Scripting Preprocessor, là một công nghệ Java cho phép các nhà phát triển tạo nội dung HTML, XML hay một số định dạng khác của trang web một cách năng động khi phản hồi yêu cầu của client. Công nghệ này cho phép người ta nhúng mã Java và một số hành động xử lý đã được định trước (pre-defined actions) vào trong nội dung tĩnh của trang.

Trước khi hiển thị ra trình duyệt, tập tin JSP phải được biên dịch thành Servlet, dùng bộ biên dịch JSP (JSP compiler). Bộ biên dịch JSP có thể tạo servlet thành mã nguồn Java trước, rồi biên dịch mã nguồn ra tập tin .class dùng bộ biên dịch Java, hoặc có thể trực tiếp tạo mã byte code cho servlet từ trang JSP.

*Perl*

Perl (Practical Extraction and Report Language) được Larry Wall xây dựng từ năm 1987, với mục đích chính là tạo ra một ngôn ngữ lập trình có khả năng chắt lọc một lượng lớn dữ liệu và cho phép xử lý dữ liệu nhằm thu được kết quả cần tìm. Cú pháp lệnh của Perl khá giống với C, từ các kí hiệu đến tên các hàm, do đó, nhiều người (đã có kinh nghiệm với C) thấy Perl dễ học. Perl khá linh hoạt và cho phép người sử dụng giải quyết với cùng một vấn đề được đặt ra theo nhiều cách khác nhau.

*Một số ngôn ngữ thực thi khác*

Ngoài ra còn một số ngôn ngữ thực thi mã nguồn ứng dụng web khác như: Python, Ruby, C#, VB.NET, …

**Lớp cơ sở dữ liệu**

Cơ sở dữ liệu (CSDL) hay Database, là một tập hợp thông tin có cấu trúc. Tuy nhiên, thuật ngữ này thường dùng trong công nghệ thông tin và nó thường được hiểu rõ hơn dưới dạng một tập hợp liên kết các dữ liệu. Dữ liệu này được duy trì dưới dạng một tập hợp các tập tin trong hệ điều hành hay được lưu trữ trong các hệ quản trị cơ sở dữ liệu.

Lớp cơ sở dữ liệu trong cấu trúc web là nơi mà ứng dụng web lưu trữ toàn bộ dữ liệu và thực hiện thao tác với nó bằng các truy vấn.

Một số hệ quản trị cơ sở dữ liệu thường gặp trong ứng dụng web:

*Oracle*

Oracle cung cấp một hệ quản trị cơ sở dữ liệu (Database Management System – DBMS) uyển chuyển: Oracle Server để lưu giữ và quản lý các thông tin dùng trong các ứng dụng. Oracle quản lý cơ sở dữ liệu với tất cả các ưu điểm của cấu trúc CSDL quan hệ, cộng thêm khả năng lưu giữ và thực thi các đối tượng CSDL như các procedure và các trigger.

*SQL Server*

SQL Server là hệ thống quản trị cơ sở dữ liệu quan hệ (Relational DataBase Management System- RDBMS), do hãng Microsoft phát triển, được cài đặt và chạy trên hệ điều hành Windows. SQL Server tỏ ra khá phổ biến và thân thiện với người dùng thông qua giao diện đồ họa trên Windows.

SQL Server sử dụng các lệnh giáo chuyển Transaction-SQL để trao đổi dữ liệu giữa Client Computer và Server Computer.

*MySQL*

MySQL là hệ quản trị cơ sở dữ liệu mã nguồn mở phổ biến nhất thế giới và được các nhà phát triển rất ưa chuộng trong quá trình phát triển ứng dụng web. Vì MySQL có tốc độ cao, ổn định và dễ sử dụng, có tính khả chuyển, hoạt động trên nhiều hệ điều hành cung cấp một hệ thống lớn các hàm tiện ích rất mạnh. Với tốc độ và tính bảo mật cao, MySQL rất thích hợp cho các ứng dụng có truy cập CSDL trên internet. MySQL miễn phí hoàn toàn nên có thể tải về MySQL từ trang chủ. Nó có nhiều phiên bản cho các hệ điều hành khác nhau: phiên bản Win32 cho các hệ điều hành dòng Windows, Linux, Mac OS X, Unix, FreeBSD, NetBSD, Novell NetWare, SGI Irix, Solaris, SunOS…

MySQL là một trong những ví dụ rất cơ bản về Hệ Quản trị Cơ sở dữ liệu quan hệ sử dụng Ngôn ngữ truy vấn có cấu trúc (SQL).

*Một số hệ quản trị cơ sở dữ liệu khác*

Ngoài ra còn một số hệ quản trị cơ sở dữ liệu khác như: PostgreSQL, Microsoft Access, Sybase, …

Việc hoạch định tốt các lớp trong cấu trúc web không những giúp người quản trị dễ vận hành mà còn chủ động trong phòng, chống các nguy cơ tấn công từ tin tặc.

## Các hiểm họa đối với thư tín điện tử

***Hiểm hoạ bị đọc lén***

Cũng như đối với các ứng dụng khác trên mạng (các phiên đăng nhập từ xa, tải thông tin sử dụng ftp, hội thoại trực tuyến, ...), thư tín điện tử cũng có thể bị đọc lén. Nhưng ai là đối tượng muốn đọc lén nội dung thư của bạn? Câu trả lời phụ thuộc vào bạn là ai, bạn đang làm gì, và ai quan tâm đến việc bạn đang làm. Dưới đây là một vài đối tượng có thể đọc lén thư của bạn.

*Chính phủ nước ngoài*

Các tổ chức tình báo quân sự nước ngoài là các đối tượng nghe trộm với những thiết bị tinh vi hiện đại nhất. Đọc trộm nội dung thư cá nhân là nghề của họ. Khi bắt đầu thời kỳ chiến tranh lạnh, mỗi năm họ đã đầu tư nhiều tỷ Đô la cho việc thu thập, biên dịch và phân tích dữ liệu của đối phương gửi qua mạng. Hiện tại khi thời kỳ chiến tranh lạnh đã kết thúc, nhưng không có gì có thể khẳng định họ không thực hiện những gì họ đã từng làm.

Mối quan hệ giữa quân đội Mỹ và các tổ chức tình báo là một một quan hệ “mờ ám”, có rất nhiều ứng dụng được xây dựng bởi quân đội Mỹ hiện đang được sử dụng trong lĩnh vực thương mại. Ở một số nước, mục tiêu thu thập tin tức của họ là nhằm vào các công ty nước ngoài, thông tin thu thập được sẽ được sử dụng làm công cụ cạnh tranh cho các công ty thuộc nước bản địa. Nhật bản và Pháp là hai nước nổi tiếng nhất trong việc “phạm tội” theo kiểu này, tất nhiên các nước phát triển khác cũng hoàn toàn có thể làm được điều đó. Ví dụ NSA đã từng bị buộc tội là có hành vi chặn các cuộc điện thoại giữa hai nước châu âu để ăn cắp thông tin và bán cho các đối tượng cạnh tranh khác.

*Chính phủ trong nước*

Việc sử dụng gián điệp công nghệ đối với công dân nước mình nhiều nhất được biết đến là các nước như Trung quốc, Bắc Triều tiên, Cuba. Đối với Pháp, chính phủ chỉ cho phép mã hoá thông tin trao đổi giữa các công dân với nhau khi thuật toán mã và khoá được cấp bởi cơ quan có thẩm quyền. Còn đối với Đài loan và Hàn quốc thì họ yêu cầu các công ty loại bỏ việc sử dụng mã hoá thông tin trong các cuộc kết nối thoại, dữ liệu, và FAX.

Trong bản thân nước Mỹ, nhiều tổ chức thuộc chính phủ cũng quan tâm đến việc đọc trộm các thông tin cá nhân được trao đổi qua thư điện tử. Chẳng hạn đối với FBI, các tổ chức dính dáng đến chính trị, ...

*Cạnh tranh thương mại*

Việc kinh doanh có thể bị do thám bởi các công ty cạnh tranh. Các thông tin đối thủ cần quan tâm ở đây có thể là danh sách khách hàng, nội dung dự án, kế hoạch triển khai, tiềm lực tài chính, ... Ví dụ Coca-Cola có thể trả hậu hĩnh cho ai biết được kế hoạch quảng cáo mới của Pepsi, hãng Ford cũng có thể làm như vậy trong việc biết được thông tin về mẫu xe mới của một hãng sản xuất xe hơi khác.

*Tội phạm*

Các đối tượng phạm tội có thể thu thập những thông tin có giá trị từ thư điện tử, đặc biệt là loại tội phạm kinh tế. Cảnh sát ở nhiều nước đã phát hiện ra việc bọ điện tử được gắn bất hợp pháp trên các kênh điện thoại nhằm giám sát và nghe trộm thông tin về số thẻ tín dụng được truyền qua đường điện thoại. Không có lý do nào để có thể nói rằng chúng không làm tương tự đối với thư tín điện tử khi các thông điệp được truyền trên mạng.

Nhiều công ty đã mở giao dịch điện tử mua bán qua mạng Internet, và đã có nhiều mặt hàng được mua bán qua mạng thông qua thẻ tín dụng. Sẽ là rất dễ dàng để xây dựng và thiết lập một ứng dụng chạy tự động quét các thông điệp trên máy tính người sử dụng nhằm tìm kiếm các thông tin về số thẻ tín dụng trong các phiên giao dịch điện tử nói trên.

*Bạn bè người thân*

Cuối cùng, chính bạn bè, người thân của bạn cũng có thể là "gián điệp". Sử dụng thuật ngữ "gián điệp" trong trường hợp này có thể là chưa được chính xác, nhưng những đối tượng trên cũng cần được quan tâm khi thư tín điện tử được sử dụng để trao đổi các thông tin riêng tư. Một ví dụ đơn giản, trong môi trường làm việc ở một văn phòng, đồng nghiệp hoàn toàn có thể quan tâm đến những thông tin cá nhân được trao đổi qua thư tín điện tử của chúng ta mà không chỉ dừng lại ở mục đích tò mò.

***Vấn đề thu thập***

Vấn đề lớn nhất khi muốn đọc một thông điệp được gửi qua đường thư tín điện tử của một ai đó là việc tìm nó giữa một biển các thông điệp thư tín điện tử khác trên mạng. Công việc này được người ta ví như việc "mò kim đáy biển". Tuy là một công việc khó khăn nhưng hiện vẫn có các cơ quan hoặc tổ chức được sinh ra để làm công việc đó. Chẳng hạn, một trong các công việc chính của NSA, NSA giám sát các luồng dữ liệu máy tính vào, ra nước Mỹ và giữa các nước khác với nhau.

Nhiệm vụ thu thập thông tin từ các thông điệp thư tín điện tử được ví như nhiệm vụ của một chàng Herculean. Năm 1994, theo thống kê dữ liệu máy tính vào ra nước Mỹ đã đạt con số nhiều gigabytes, với hàng tỷ thông điệp được trao đổi trong một tháng. Trong đó gồm thư tín điện tử, thông tin đăng nhập từ xa, dịch vụ truyền tệp, dữ liệu "chat" thời gian thực, ... Để lưu trữ được lượng dữ liệu trên đã là một công việc lớn chứ chưa nói gì đến việc đọc và phân tích chúng.

Tuy nhiên đối với các thông tin cần quan tâm, các máy tính có thể thực hiện việc sàng lọc từ dòng dữ liệu trong thời gian thực. NSA hoàn toàn có thể thực hiện việc đưa luồng dữ liệu vào ra nước Mỹ vào một hệ thống máy tính mạnh, hệ thống máy tính này sẽ thực hiện việc tìm kiếm dữ liệu mà NSA quan tâm. Hệ thống máy tính này có thể tìm kiếm dữ liệu theo từ khoá, giả sử các thông điệp thư tín điện tử có chứa từ khoá "nuclear" (nguyên tử), "cryptography" (mật mã), hay "assassination" (cuộc ám sát), sẽ được lưu giữ lại phục vụ cho mục đích phân tích sau.

Ngoài ra còn rất nhiều công nghệ khác được hệ thống máy tính của NSA sử dụng. Họ có thể tìm kiếm dữ liệu từ một cá nhân hoặc một tổ chức cụ thể. Họ cũng có thể tìm kiếm dữ liệu theo một cấu trúc cho trước. Tóm lại NSA được đầu tư rất nhiều tiền cho vấn đề này, họ đã và đang thực hiện công việc trên trong một thời gian dài.

Điều quan trọng nhất là họ thực hiện công việc trên trong thời gian thực, và không nhiều lắm dữ liệu được lưu. Họ hy vọng rằng dữ liệu mà họ thu thập trong ngày nào sẽ được phân tích luôn trong ngày đó. Việc thu thập dữ liệu sẽ trở thành vô giá trị nếu dữ liệu đó không được phân tích, bởi vậy vấn đề khăn chính là việc phân tích dữ liệu. NSA có thể kết hợp rất nhiều công nghệ nhằm phân tích dữ liệu mà họ quan tâm, như mối quan hệ giữa từ khoá nói lên dữ liệu cần tìm, đối tượng gửi nhận thông tin, ...

***Phân tích đường truyền***

Trong trường hợp nội dung thư được mã hoá, đối tượng đọc trộm (NSA chẳng hạn) không thể đọc nội dung thư điện tử, họ có thể thu thập được một lượng thông tin không nhỏ thông qua việc phân tích đường truyền.

Việc phân tích đường truyền dựa vào một trong các yếu tố như: bạn gửi thư điện tử cho ai, bạn nhận thư điện tử từ ai, độ dài của các thông điệp thư điện tử, hoặc khi nào thư điện tử được gửi. Có rất nhiều thông tin ẩn chứa trong các yếu tố kiểu như vậy nếu họ biết cách khai thác.

Trước hết chúng ta hãy thử tìm hiểu lĩnh vực cung cấp dịch vụ điện thoại. Hầu hết các quốc gia châu Âu không ghi chiết khoản mục trong các hoá đơn điện thoại như đối với các công ty của Mỹ. Các hoá đơn điện thoại ở châu Âu chỉ liệt kê số lượng cuộc đàm thoại đã sử dụng qua một thuê bao cụ thể, nhưng không ghi lại thời điểm cũng như địa điểm của các cuộc đàm thoại đó. Đối với các hoá đơn thanh toán điện thoại của Mỹ, trong đó liệt kê chi tiết tất cả các cuộc đàm thoại đối với một số thuê bao: thời điểm thực hiện, số được gọi đến, và thời lượng cuộc gọi. Từ những thông tin các cuộc đàm thoại, các cơ quan có chức năng của Mỹ có thể phân loại các đối tượng cần theo dõi hoặc đưa vào danh sách các đối tượng cần đề phòng.

Tương tự như vậy đối với các thông điệp thư tín điện tử. Thậm chí khi các thông điệp thư tín điện tử đã được mã hoá, phần đầu của thông điệp thư tín điện tử bao giờ cũng thể hiện rõ đối tượng gửi, đối tượng nhận, thời điểm gửi, và độ dài của thông điệp. Trên thực tế đã có những dịch vụ thư tín điện tử “ẩn danh”, nhằm che dấu đi những thông tin chúng ta vừa liệt kê ở trên. Tuy nhiên theo các nhà phân tích về lĩnh vực này trên thế giới đã cho rằng điều đó chẳng có nghĩa lý gì đối với các đối tượng nghe trộm cỡ NSA.

Một ví dụ cụ thể hơn, giả sử Eve nghi ngờ Alice là người ủng hộ chủ nghĩa khủng bố. Trong khi đó tất cả thư tín điện tử của Alice được cô ấy mã hoá, bởi vậy Eve không thể đọc được nội dung của các thông điệp thư tín điện tử được gửi nhận bởi Alice. Tuy nhiên, Eve có thể thu thập tất cả các thông tin trên đường truyền của Alice. Eve biết tất cả các địa chỉ thư điện tử của những người mà Alice thường liên lạc. Alice thường gửi các thông điệp thư tín điện tử dài cho một người có tên là Bob, người thường phúc đáp ngay sau đó với một thông điệp rất ngắn. Có thể cô ấy đã gửi Bob các mệnh lệnh và anh ta phúc đáp lại việc đã nhận được các lệnh đó. Một ngày nào đó bỗng dưng có một bước nhảy vọt trong việc trao đổi thư điện tử giữa Alice và Bob. Có thể họ đang lập một kế hoạch gì đó. Và sau đó là sự im lặng, không có một thông điệp thư điện tử nào được trao đổi qua lại giữa họ. Ngày tiếp theo toà nhà chính phủ bị đánh bom. Điều này đã đủ làm bằng chứng để bắt giữ họ chưa còn tuỳ thuộc vào nhiều bằng chứng khác, nhưng ít nhất chúng đã đem lại cho các cơ quan quan tâm đến lĩnh vực này không ít thông tin quý giá.

Khủng bố không phải là đối tượng duy nhất bị theo dõi thông qua việc phân tích đường truyền. Việc phân tích đường truyền trao đổi thông điệp thư tín điện tử cũng là một công cụ để FBI căn cứ trong việc điều tra tội phạm buôn bán ma tuý.

Trong lĩnh vực kinh tế xã hội, một công ty sẽ nghĩ sao khi một thành viên trong công ty đó thường xuyên liên lạc thư điện tử với một đối thủ cạnh tranh. Điều gì sẽ xảy ra nếu một người hay ghen nhận thấy vợ hoặc chồng mình thường xuyên liên hệ với “đối thủ tiềm năng” thông qua thư điện tử.

Tóm lại việc phân tích đường truyền thư điện tử là một công cụ thông minh trong việc ăn cắp thông tin cá nhân.

***Giả mạo***

Giả mạo là một vấn đề an toàn khác trên mạng máy tính nói chung. Khái niệm ngắn nhất và giả mạo là việc người này giả danh là một người khác. Việc giả mạo có thể xuất phát từ mục đích trêu đùa, làm mất danh dự, bôi nhọ người khác hoặc là công cụ để lừa gạt.

Hàng ngày có rất nhiều thông điệp thư tín được gửi một cách tự động đến hộp thư của người sử dụng trên mạng Internet, với chủ đề kiểu như “tôi là người thích làm phiền người khác và tôi tự hào về điều đó” hoặc với chủ đề như một khẩu hiệu trong việc phân biệt chủng tộc, phân biệt giới tính. Nội dung của các thông điệp thư tín điện tử này hoàn toàn không có ý nghĩa gì. Sau đó một thời gian lại có một thư khác cũng xuất phát từ cùng một tài khoản với lời xin lỗi về việc đã gửi thư điện tử thứ nhất. Nói chung không nên tin vào bất kỳ điều gì trong các thông điệp thư tín kiểu như vậy, đấy chỉ là một trò trêu đùa trên mạng.

Một ví dụ khác, Eve muốn bôi nhọ Alice. Cô ta viết một thư điện tử buộc tội một ai đó, viết tên của Alice ở cuối thư, giả mạo thông tin cá nhân của Alice trên phần tiêu đề của thư (điều này được thực hiện một cách dễ dàng đối với các tin tặc), sau đó cô ta gửi một bản copy tới một tạp chí nào đó, như The New York Times chẳng hạn.

Một kiểu giả mạo khác chúng ta có thể lấy ví dụ như kiểu tấn công của kẻ thứ ba trong mật mã. Ví dụ, Bob và Alice hợp tác với nhau trong một dự án nào đó, và họ thương xuyên trao đổi thông tin với nhau qua thư điện tử. Eve giả danh là Bob gửi thư điện tử cho Alice và nói rằng tài khoản thư điện tử trước đây đã bị huỷ bỏ. Tương tự như vậy đối với Bob và nếu cả Bob và Alice đều tin vào nội dung thư điện tử nhận được thì mọi liên hệ giữa Alice và Bob được thực hiện thông qua người thứ ba là Eve. Khi đó Eve sẽ biết mọi thông tin về dự án mà Bob và Alice đang hợp tác. Eve sẽ là người đánh cắp thông tin trao đổi giữ Bob và Alice chừng nào Bob và Alice chưa trao đổi trực tiếp hoặc thông qua điện thoại.

Hiểm hoạ mạo danh có thể được khắc phục thông qua việc sử dụng chữ ký điện tử. Với chữ ký điện tử Alice (trong ví dụ trên) hoàn toàn có thể kiểm tra được những thông điệp thư tín điện tử nào là thật sự của Bob. Và cũng không ai có thể mạo danh Alice để gửi các thông điệp điện tử cho người khác.

***Bom thư***

Nếu bạn đang sử dụng thư điện tử, bạn có thể đã từng nhận được một số thông điệp thư điện tử được gửi một cách tự nguyện từ một địa chỉ nào đó tới mà chưa được sự cho phép của bạn, những thông điệp thư điện tử đó được gọi là spam. Spam là một kiểu thư rác trên Internet, spam được sử dụng cho rất nhiều mục đích: quảng cáo, quấy rối, ...

Nếu là một người mới sử dụng Internet có thể bạn chỉ nhận được một số ít thông điệp điện tử không mong muốn như trên. Nhưng khi bạn đã sử dụng Internet được một vài năm bạn có thể đã cảm thấy rất khó chịu khi nhận được hàng loạt thư điện tử mà mình không hề mong muốn.

Dưới đây là một số kiểu thư điện tử thường xuyên xuất hiện trong hộp thư của bạn:

* Các thông điệp điện tử được gửi từ các công ty thương mại nào đó mà bạn chưa hề có mối quan hệ trước đây.
* Thư điện tử có mục đích quảng cáo cho các sản phẩm hoặc dịch vụ bất hợp pháp, mờ ám hoặc thậm chí là có mục đích đánh lừa người nhận.
* Các thư điện tử được gửi từ một địa chỉ không rõ ràng.
* Các thư không hề có địa chỉ để người nhận có thể phúc đáp

Nếu bạn đã từng nhận được một mẩu bom thư nào đó, có thể bạn đã có cảm giác bối rối, và tự mình đặt ra những câu hỏi như: thông điệp này là gì vậy? Nó được gửi từ đâu đến và bằng cách nào những người gửi thư có được địa chỉ hộp thư của mình?

Khi những băn khoăn của mình vừa qua đi thì bạn đã nhận được liên tiếp các thư rác tiếp theo, và như vậy chúng đã gây nên sự bực mình cho bạn. Có thể, bạn sẽ viết thư than phiền với người gửi thư rác, nhưng sự bực mình của bạn sẽ tăng lên khi biết thư điện tử than phiền của mình sẽ không đến được đối tượng mình cần gửi, vì kẻ gửi thư rác thường nguỵ trang hoặc dựng giả một hộp thư nào đó khi gửi cho bạn.

Một số loại bom thư:

* Thư điện tử thương mại tự nguyện (UCE - Unsolicited Commercial Email): là các thông điệp thư điện tử mà người sử dụng nhận được ngoài ý muốn, với nội dung nhằm quản cáo cho một sản phẩm hay một dịch vụ nào đó. Loại bom thư này còn được gọi là "Junk mail".
* Thư điện tử gửi hàng loạt (UBE - Unsolicited Bulk Email): được biết đến như các thông điệp điện tử được gửi với số lượng lớn cho hàng nghìn thậm chí hàng triệu người nhận. UBE có thể được sử dụng cho mục đích thương mại, trong trường hợp đó nó cũng là UCE. Nhưng nó cũng có thể được sử dụng cho nhiều mục tiêu khác, như vận động bầu cử trong lĩnh vực chính trị, hay chỉ đơn giản là gây rối hệ thống thư điện tử.
* Các thông điệp thư điện tử kiếm tiền nhanh (MMF - Make Money Fast): thường các thông điệp này là một chuỗi các thư cùng một mẫu. Nội dung của các thông điệp thư điện tử kiểu này gợi ý người nhận rằng họ có thể trở nên giàu có nếu thực hiện theo các bước như:
* *Hãy gửi tiền cho người có tên đầu tiên trong danh sách (danh sách được gửi kèm theo thư)*
* *Loại bỏ tên của người đó, bổ sung tên của mình vào cuối danh sách và chuyển thông điệp đó cho người khác.*

## Các lỗ hổng, điểm yếu thường gặp đối với ứng dụng web

Trong phần này, chúng ta sẽ nói về các lỗ hổng liên quan tới ứng dụng Web và các kỹ thuật thực hiện đánh giá an toàn cho các ứng dụng Web. Đồng thời chúng ta cũng sẽ tìm hiểu về một số công cụ hỗ trợ liên quan sử dụng trong quá trình thực hiện đánh giá.

Hiện nay có rất nhiều các phương pháp sử dụng để đánh giá an toàn cho ứng dụng Web, nhưng chúng ta sẽ tập trung vào phương pháp đánh giá của OWASP. Trước khi đi vào cụ thể phương pháp thực hiện đánh giá, chúng ta sẽ nói sơ lược về các lỗ hổng điển hình trên ứng dụng Web

OWASP Top 10 là danh sách được OWASP tổng hợp và công bố theo từng năm, nhằm đưa ra các cảnh báo rủi ro an ninh của ứng dụng web một cách ngắn gọn và xúc tích, giúp các doanh nghiệp, cá nhân xây dựng, phát triển, hay đánh giá các ứng dụng web có thể tự đưa ra được các giải pháp phù hợp, nâng cao bảo mật thông tin. Danh sách này luôn được thay đổi và cập nhật liên tục, do sự thay đổi về các tác động ảnh hưởng của các lỗ hổng.

**Injection:** Sai sót trong nhập liệu, chẳng hạn như SQL injection, OS injection hay LDAP injection… Điều này xảy ra khi các thông tin sai lệch được đưa vào cùng với các biến dữ liệu đầu vào như 1 phần của lệnh hay câu truy vấn. Kẻ tấn công có thể lợi dụng sơ hở này để thực hiện các lệnh không mong muốn hay truy cập các dữ liệu bất hợp pháp.

**Broken Authentication and Session Management:** Xác thực hay quản lý phiên thiếu chính xác. Sơ hở này cho phép kẻ tấn công có thể lợi dụng để đạt được mật khẩu, khóa hay phiên làm việc, từ đó mạo danh phiên làm việc và danh tính của người dùng thông thường.

**Cross-Site Scripting (XSS):** Sai sót trong kiểm duyệt nội dung đầu vào cũng dẫn đến rủi ro này. Các dữ liệu bất hợp pháp được gửi đến trình duyệt web mà ko cần sự xác nhận thông thường. Nó cho phép kẻ tấn công thực thi các kịch bản trên trình duyệt web của nạn nhân làm thay đổi nội dung trang web, chuyển hướng nạn nhân hay đánh cắp phiên làm việc được lưu trên trình duyệt.

**Insecure Direct Object References:** Điều này xảy ra thì nhà phát triển cho thấy có các tham chiếu trực tiếp đến một đối tượng nội bộ hay của người dùng khác, ví dụ như một tập tin, thư mục, hay cơ sở dữ liệu quan trọng, mà ko có sự kiểm tra hay bảo vệ an toàn cần thiết. Điều này cho phép kẻ tấn công có thể truy cập các tài liệu này một cách trái phép.

**Security Misconfiguration:** Một hệ thống bảo mât tốt là hệ thống triển khai cho khung ứng dụng, máy chủ ứng dụng, máy chủ cơ sở dữ liệu, nền tảng… các phương phảp bảo mật cần thiết, thống nhất và liên kết với nhau. Điều này nhằm tránh những nguy cơ bị khai thác vào ứng dụng, ví dụ để lộ ra những thông tin quan trọng khi trao đổi các gói tin.

**Sensitive Data Exposure:** Các dữ liệu nhạy cảm không được lưu trữ và bảo vệ cẩn thận, dẫn đến khi bị kẻ tấn công khai thác gây ra những ảnh hưởng to lớn cho hệ thống máy chủ, doanh nghiệp, khách hàng. Ví dụ như việc lưu trữ thẻ tín dụng mà ko thông qua các khâu mã hóa, hay các gói tin TLS bị bẻ khóa và nghe lén thông qua lỗ hổng CRIME.

**Missing Function Level Access Control:** Thiếu các điều khoản trong việc phân quyền quản trị các mức, dẫn đến việc kẻ tấn công có thể lợi dụng và truy ra các điểm yếu trên hệ thống, hay lợi dụng để leo thang đặc quyền.

**Cross-Site Request Forgery (CSRF):** Lợi dụng sơ hở của nạn nhân, kẻ tấn công có thể lừa nạn nhân thực hiện các hành động nguy hiểm mà nạn nhân không hề hay biết, ví dụ như chuyển tiền từ tài khoản nạn nhân sáng tài khoản kẻ tấn công, thông qua các lỗ hổng XSS.

**Using Known Vulnerable Components:** Sử dụng các thư viện, plugin, module… có chứa các lỗ hổng đã được công khai, dễ dàng dẫn đến việc bị kẻ tấn công lợi dụng để tấn công vào hệ thống một cách nhanh chóng.

**Unvalidated Redirects and Forwards:** Chuyển hướng không an toàn người dùng đến một đường dẫn bên ngoài có thể bị kẻ tấn công lợi dụng để chuyển hướng nạn nhân đến một trang đích được chuẩn bị sẵn của kẻ tấn công.

## Quy trình thực hiện kiểm tra các lỗ hổng ứng dụng Web

Quy trình kiểm tra các lỗ hổng, điểm yếu của hệ thống ứng dụng web cũng như thư điện tử tuân theo tiêu chuẩn kiểm định của OWASP và được tiến hành tuần tự theo các bước nhằm thu thập được tối đa thông tin và khai thác thành công được đối tượng. Gồm có:

*1. Thu thập và khảo sát thông tin*

*2. Kiểm tra quản lý cấu hình*

*3. Kiểm tra business logic*

*4. Kiểm tra cơ chế xác thực*

*5. Kiểm tra việc ủy quyền*

*6. Kiểm tra quản lý phiên giao dịch*

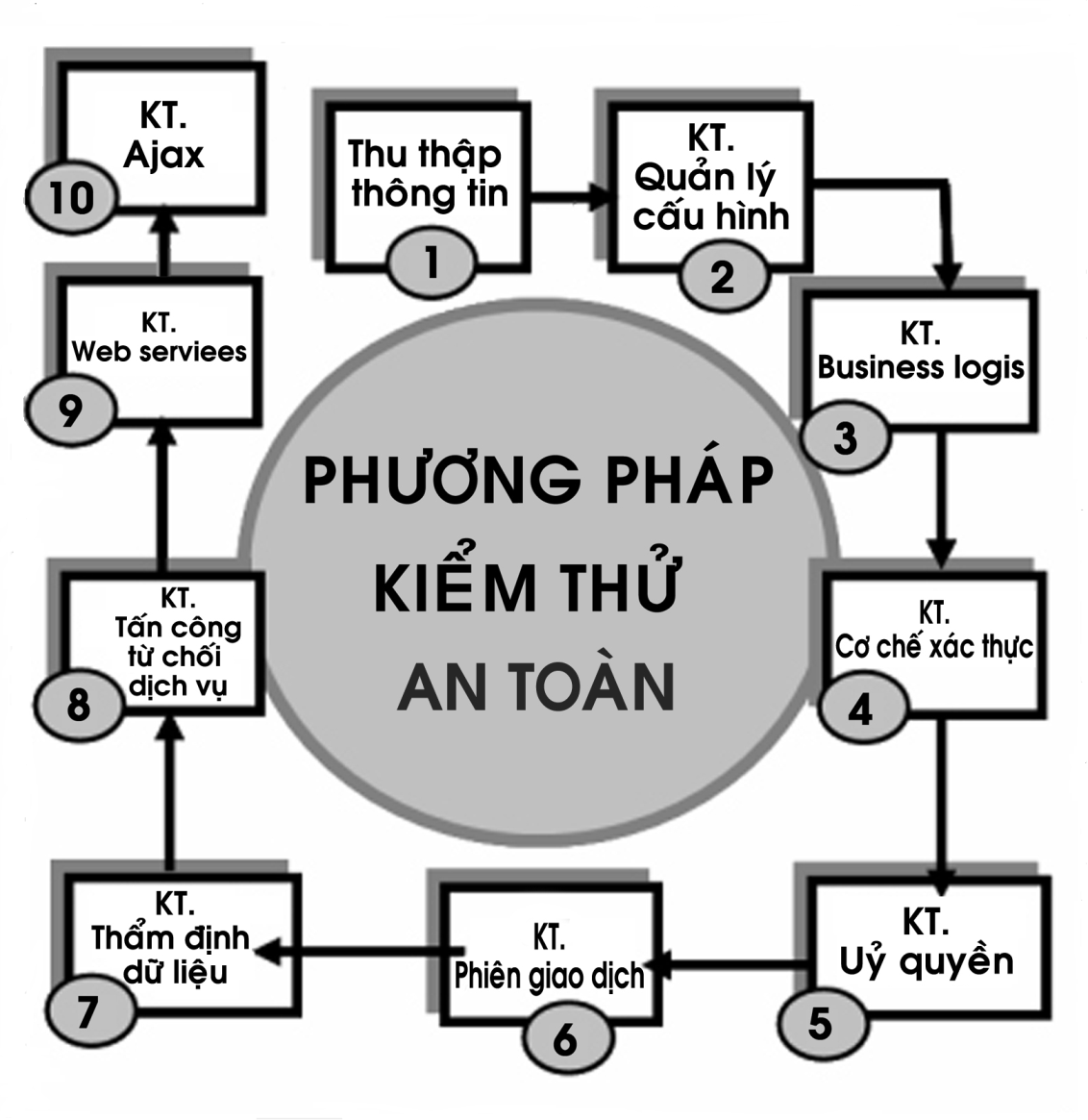
*7. Kiểm tra các dữ liệu đầu vào*

*8. Kiểm tra khả năng tấn công từ chối dịch vụ*

*9. Kiểm tra web services*

*10. Kiểm tra AJAX*

Hình dưới đây mô tả đầy đủ về quy trình kiểm thử của OWASP:



*Hình 7.2: Quy trình ki****ể****m thử OWASP*

* **Kiểm tra quản lý cấu hình**

Thường xuyên phân tích kiến trúc cơ sở hạ thầng và topo mạng có thể tiết lộ rất nhiều thông tin về hệ thống cũng như vậy việc phân tích cơ sở hạ tầng và kiến trúc của website có thể giúp xác định rất nhiều yếu tố về một ứng dụng web như: Một số thông tin về mã nguồn, các phương pháp xử lý mà HTTP cho phép, chức năng, phương pháp xác thực, và cấu hình cơ sở…

*Kiểm tra giao thức SSL/TLS*

Như đã biết Htttp là giao thức được truyền dưới dạng clear-text và để đảm bảo an toàn cho truyền dữ liệu qua http thì người ta sử dụng SSL/TLS. SSL và TLS là hai giao thức cung cấp, sự hỗ trợ tạo ra các kênh truyền dữ liệu an toàn để bảo vệ tính bảo mật và xác thực của thông tin được truyền đi.

Có 1 điểm thú vị là ngày nay các website đã phần nào áp dụng SSL/TLS nhằm đảm bảo an toàn cho website của mình. Nhưng ngoài những việc kiểm tra SSL/TLS mục đích là kiểm tra hệ thống đã sử dụng các thuật toán mã hóa đủ mạnh, đúng chuẩn để bảo đảm an toàn chưa.... mà còn phải kiểm tra vị trí của SSL/TLS trong mô hình OSI bởi SSL/TLS còn phải hoạt động khớp với các giao thức trên nó. Bởi khai thác lỗ hổng này thì kẻ tấn công có thể chèn thêm một đoạn plaintext bất kỳ vào TLS/SSL encrypted stream giữa client và server mà cả client và server đều không thể phát hiện được. Vì vậy cần phải kiểm tra độ tin cậy của giao thức SSL/TLS.

*Dò tìm cơ sở dữ liệu*

Bất cứ website nào cũng cần phải có cơ sở dữ liệu để lưu trữ dữ liệu các bản ghi phòng trừ các trường hợp backup.....Trong cấu hình máy chủ cơ sở dữ liệu, người quản trị có thể không lường trước được các tấn công bảo mật và thành phần (module) DB listerner có thể lộ ra các thông tin quan trọng nhằm giúp cho chuyên gia đánh giá tìm ra các lỗ hổng đã công bố về phần mềm cơ sở dữ liệu. Sử dụng các công cụ kiểm tra và các thông tin thu thập được từ các bước khảo sát trước, xác định cơ sở dữ liệu của website, không những thế những thông tin về phiên bản loại cơ sở dữ liệu, cổng lắng nghe..... còn giúp chuyên gia kiểm thử xâm nhập phát hiện được lỗ hổng nào có thể khai thác tương ứng cơ sở dữ liệu hiện dùng.

*Phân tích cách thức ứng dụng xử lý dạng tập tin*

Đuôi của các tập tin trên máy chủ Web cho phép chuyên gia đánh giá nhận dạng được công nghệ trang Web sử dụng. Ví dụ đuôi jsp và asp cho phép chuyên gia đánh giá biết được ứng dụng Web dựa trên nền tảng Sun Java hoặc Microsoft. Thực hiện gửi các yêu cầu tải về (download) các trang có đuôi như sau đến máy chủ web nhằm tìm ra tập tin có thể tải về được để lấy thông tin: .java, .txt: text file, .pdf: PDF documents, .doc, .rtf, .xls, .ppt,.bak, .old…

Các tập tin thừa, tập tin lưu trữ, tập tin không được tham chiếu, có thể đọc hoặc tải về (download) là nguồn thông tin quan trọng cho chuyên gia đánh giá. Những tập tin này có thể vô tình chứa những thông tin nhạy cảm như nguồn của ứng dụng, đường dẫn ứng dụng cũng như các thông tin nhạy cảm như mật khẩu của cơ sở dữ liệu... Thao tác này nhằm thực hiện yêu cầu với các tài nguyên hiện có và không có, sao đó so sánh sự phản hồi từ phía server để nhận diện ra sự phải hồi nào đối với server là không có. Bằng cách quan sát tất cả các nội dung client side code, sử dụng phương pháp fuzzing.....fuzzing: là một chương trình được cả các nhà thiết kế phần mềm và các nhà nghiên cứu bảo mật sử dụng nhằm tìm ra các lỗi bằng cách chèn dữ liệu vào các parsers nhằm phát hiện lỗi chương trình.

*Kiểm tra phương thức HTTP và XST*

Trong quá trình hoạt động giao thức http có sử dụng nhiều phương phức để hỗ trợ việc truyền dữ liệu từ webserver đến client hay ngược lại, upload, xoá bỏ cập nhật trạng thái như : HEAD, GET, POST, PUT, DELETE, TRACE, OPTIONS, CONNECT. Việc kiểm tra xem web server có hỗ trợ 2 phương thức là TRACE và HEAD hay không? Nếu có, cần kiểm tra xem có khả năng bị tấn công XST hay không. Các HTTP method có thể gây nguy hiểm như:

PUT: phương thức này cho phép client upload file lên server, lợi dụng phương thức này kẻ tấn công có thể upload lên những file có chứa mã độc hại gây nguy hiểm cho hệ thống

DELETE: phương thức này cho phép client có thể xoá bỏ file trên webserver. Khai thác phương thức này dẫn đến việc thay đổi nội dung những file quan trọng bị xoá bỏ gắn đến một cuộc tấn công dos.

CONNECT : phương thức này cho phép client có thể sử dụng webserver như là 1 porxy.

TRACE : phương thức này sẽ phản ánh lại cho client bất cứ những gì đã gửi cho server nhằm mục đích gỡ lỗi nhưng có thể gây nguy hiểm bởi 1 cuộc tấn công Tracing Cross Site.

Một số các phương thức này có thể có khả năng gây ra một nguy cơ bảo mật cho một ứng dụng web, vì chúng cho phép kẻ tấn công sửa đổi các tập tin được lưu trữ trên máy chủ web, đánh cắp các thông tin của người sử dụng ......

Bằng cách sử dụng một số công cụ như netcat, nexpose... hỗ trợ tiến hành gửi đến máy chủ web các request theo các phương thức trên để lợi dụng khả năng mắc lỗi.

* **Kiểm tra business logic**

Business logic bao gồm:

* Các luật tác vụ trên ứng dụng Web cho người dùng
* Các luồng tác vụ (Workflows), luân chuyển dữ liệu.
* **Kiểm tra cơ chế xác thực**

Xác thực là cơ chế xác định chủ thể khi đăng nhập vào hệ thống. Cơ chế này chính là phần đăng nhập (log-on) vào ứng dụng. Kiểm tra cơ chế xác thực dựa trên các phân tích cơ chế hoạt động của thành phần đăng nhập (module log-on) trong ứng dụng Web để tìm ra các điểm yếu.

*Kiểm tra phương thức truyền dữ liệu*

Đánh giá xem các phương thức truyền dữ liệu có bảo đảm an toàn thông tin. Có nghĩa là việc thử nghiệm xem việc xác minh dữ liệu xác thực của người sử dụng có được mã hoá hay không để tránh bị các tấn công chặn bắt dữ liệu bằng cách sử đụng giao thức HTTPS, SSL/TLS.....

*Kiểm tra việc thu thập thông tin người dùng*

Kiểm tra việc tìm kiếm thông tin về các người dùng (user) trong hệ thống

*Kiểm tra các tài khoản mặc định và dễ đoán*

Kiểm tra việc tìm kiếm thông tin về các người dùng (user) trong hệ thống. Việc một hệ thống còn tồn tại những tài khoản mặc định là hoàn toàn có thể xẩy ra. Bởi trong quá trình thiết kế, những dịch vụ, tài khoản không sử dụng nhưng không bị disable gây mất an toàn cho hệ thống. Các tài khoản như admin, root, administrator, guest, super.......

*Tấn công vét cạn*

Khi các kiểm tra tài khoản mặc định không thành công, tiếp tục sử dụng phương pháp vét cạn nhằm kiểm tra hệ thống xác thực. Ở bước này tiến hành kiểm tra một website có sử dụng biện pháp nào để chống lại tấn công vét cạn như đăng nhập bao nhiêu lần thì tài khoản bị xoá.... nhưng kiểu tấn công vét cạn như:

* Dictionary attacks
* Search attacks
* Rule-based search attacks
* Vượt qua tầng xác thực

Sử dụng các phương pháp khác để vượt qua tầng xác thực như tìm cách truy cập vào tài nguyên trực tiếp không thông qua cửa xác thực. Bằng cách như xác thực bằng tay trực tiếp vào các trang yêu cầu cần xác thực, thay đổi các tham số và gửi đến trình duyệt ..... Để tìm cách vượt qua phần xác thực của một ứng dụng web thông thường sử dụng cách sau:

* Gửi yêu cầu kết nối trực tiếp (Direct page request hay forced browsing)
* Sửa đổi thông số Parameter (Parameter Modification)
* Đoán ID của phiên (Session ID Prediction )
* Tấn công SQL Injection
* Kiểm tra cơ chế nhớ mật khẩu và tạo lại mật khẩu

Thực hiện kiểm tra cơ chế ứng dụng quản lý quy trình “quên mật khẩu”. Ngoài ra, cũng kiểm tra cơ chế nhớ mật khẩu trên trình duyệt.

* Vận hành chức năng lưu mật khẩu đăng nhập
* Quan sát sự thay đổi về cookies khi thực hiện chức năng này
* Việc lưu trữ thường được mã hoá, thử bằng nhiều username, passoword giống nhau.

*Kiểm tra cơ chế nhớ mật khẩu:*

* Nếu như ứng dụng có chức năng lưu mật khẩu đăng nhập thì hãy quan sát cách thức vận hành của chức năng này.
* Quan sát sự thay đổi về cookies khi thực hiện chức năng và khả năng dự đoán đến chúng.
* Dữ liệu cho việc lưu trữ này thường là mã hóa, do vậy hãy thử chức năng với các username hoặc password tương tự nhau để xem liệu có khả năng giải mã các mã hóa này.
* Dựa trên kết quả quan sát mà có thể thay đổi nội dung cookies để đóng giả username khác trong ứng dụng.

*Kiểm tra cơ chế tạo lại mật khẩu:*

* Xác định liệu ứng dụng có cung cấp chức năng khôi phục lại mật khẩu cho username không. Nếu có thì hãy thử tìm hiểu quá trình khôi phục mật khẩu mà ứng dụng cung cấp là như thế nào.
* Nếu như ứng dụng sử dụng cơ chế với các câu hỏi bảo mật thì hãy xem liệu rằng user có thể thiết lập hoặc lựa chọn các câu hỏi này hay không
* Nếu như ứng dụng sử dụng chức năng password hint thì cũng thực hiện tương tự như đối với câu hỏi bảo mật.
* Nếu như chức năng đề cập đến việc gửi mail đến user để hoàn tất việc khôi phục mật khẩu thì hãy xác định các điểm yếu có thể xảy ra đối với các URL links mà ứng dụng gửi đến. Thực hiện đánh giá các URL links này có khả năng dự đoán các links hay không?

*Kiểm tra cơ chế đăng xuất*

Thực hiện kiểm tra việc đăng xuất và quản lý bộ nhớ đệm (cache) để đảm bảo hai cơ chế trên không làm thất thoát thông tin nhạy cảm. Đối với những hệ thống áp dụng Single Sign On việc đăng nhập một lần luôn cần kiểm tra cơ chết đăng xuất một lần, bởi khi sử dụng đa ứng dụng, việc đăng xuất không phải một lần gây rò rỉ thông tin nhạy cảm.

* **Kiểm tra quản lý phiên giao dịch**

Các ứng dụng web thực hiện cơ chế khác nhau để lưu trữ và xác nhận các thông tin cho một khoảng thời gian xác định trước. Những cơ chế này được gọi là quản lý nhiên, nhằm tăng sự dễ dàng và thân thiện của ứng dụng đối với người dùng. Tuy nhiên, kẻ tấn công có thể truy cập vào tài khoản người dùng mà không cần cung cấp những thông tin chính xác. Trong bước này cần phải hiểu được quá trình sinh token, để kiểm tra xem cookie và các security token có được tạo ra một cách an toàn, có thể đoán trước đựơc hay không. Một kẻ tấn công nếu chiếm hoặc giả mạo được cookie có thể dễ dàng chiếm (hijacking) phiên của người khác. Quá trình kiểm tra gồm:

- Cookie có được tag là Secure hay không

- Cookie được truyền qua một cách một kênh mã hóa

- Cookie có bắt buộc phải truyền qua kênh mã hóa an toàn không.

- Có Expires time trong cookie hay không

- Các tham số HTTP/1.1 Cache-Control và HTTP/1.0 Cache-Control.

- Đối với các trang quản trị người dùng yêu cầu No Cache.

- Kiểm tra quá trình tạo cookie, lưu ý đến quá trình sinh cookie có

- phải là sinh ngẫu nhiên hay không (hạn chế đoán cookie)

- Kiểm tra khả năng giãi mã ngược cookie (revensing cookie)

- …

*Phân tích cơ chế quản lý phiên giao dịch*

Hiểu rõ cơ chế mà ứng dụng triển khai trong việc quản lý phiên và trạng thái, xác định ứng dụng có sử dụng token hoặc các phương thức nào khác trong việc xác định yêu cầu của từng người sử dụng.Thực hiện kiểm tra token nào thuộc về ứng dụng có thể thực hiện bằng cách thực hiện các yêu cầu liên quan đến phiên như tài sản..... Trong bước này, thực hiện xem xét các vấn đề:

- Cookie được truyền qua kênh an toàn (ví dụ như https chẳng hạn)

- Có sử dụng HttpOnly hay không.

- Tên miền (domain) sử dụng có phải tên miền con (sub-domain) hay không. Nếu là tên miền con có chung, hoặc liên quan gì đến cookie của tên miền chính hay không.

- Path: quy định đường dẫn mà URL có tác dụng.

- Expires: thời gian mà cookie có hiệu lực

*Phân tích cơ chế quản lý token*

Sinh ra và thu thập một số lượng token đối với các xác thực thành công. Dựa vào quá trình thu thập token và thực hiện phân tích token để hiểu token loại bỏ dữ liệu không liên quan, phân tích các thành phần trong token, những điểm cố định... từ đó nhận biết khả năng đoán token, dẫn đến cơ hội cho kẻ tấn công mạo danh nạn nhân truy cập ứng dụng bất hợp pháp.. Như vây, điều quan trọng là phải bảo vệ những thông tin, token này – đặc biệt là trong quá trình giao tiếp giữa trình duyệt và ứng dụng web. Ở bước này, tập trung vào kiểm tra:

- Giao thức (protocol) được sử dụng (HTTP hay HTTPS)

- HTTP Headers

- Message Body

Mỗi thông tin được trao đổi qua giữa máy khách (client) và ứng dụng web, một đường truyền an toàn là cần thiết để gửi các thông tin nhạy cảm này. Các bước kiểm tra bao gồm:

- Kiểm tra mã hóa, SSL, tái sử dụng các security token: Để chống tại tấn công nghe lén, ứng dụng cần phải hỗ trợ SSL, cũng như các giải pháp tunnel hoặc mã hóa. Session ID là thông tin của riêng người dùng, do đó, phải đảm bảo session ID không được truy cập bởi bất kỳ ai khác. Đơn giản nhất, sẽ thử thay thể http bằng https, cũng như xem xét HTTP header và response để xem các tham số, thành phần nhạy cảm (username, password) có được mã hóa hay không.

- Kiểm tra Proxies & Caching: đối với các doanh nghiệp, ISP, proxy thường đựơc triển khai. Proxy được triển khai để điều khiển các luồng dữ liệu. Session ID là một tham số nhạy cảm, không nên được lưu trữ và gửi không mã hóa. Quá trình kiểm tra bao gồm:

- Kiểm tra HTTP header: Cache-Control: max-age=0 hoặc Cache-Control: no-cache.

- Kiểm tra GET POST

- Kiểm tra các thành phần được gửi đi, gồm:

- Session ID có đựơc gửi đi không? (GET POST hidden form)

- Session ID có được mã hóa không?

- Có thể làm cho ứng dụng gửi Session ID chưa mã hóa (thay đổi https bằng http chẳng hạn)

*Kiểm tra CSRF*

Nếu chị dựa vào mỗi HTTP cookies thì website sẽ có nguy cơ bị lỗi CSRF. Ở bước này cần phải quan sát chức năng cốt lỗi của ứng dụng và xác định các yêu cầu thực hiện với các dữ liệu nhạy cảm, nếu như kẻ tấn công có thể xác định được toàn bộ tham số đối với các yêu cầu ( cho dù không thể xác định HTTP cookie) thì ứng dụng đó vẫn lỗi CSRF. Tiến hành kiểm tra các tác vụ trong phần “Thành Viên” của cả 3 website để tìm các tác vụ sử dụng các request dạng GET để thực thi trên hệ thống. Tuy nhiên trên hệ thống các tác vụ quan trọng đều sử dụng các request dạng POST, và một số tác vụ vẫn sử dụng dạng GET ở phần đầu tuy nhiên có cơ chế captcha xác nhận. Do vậy kẻ tấn công không thể lợi dụng để tấn công kiểu CSRF (giả mạo các request gửi đến trong phiên làm việc của người dùng và khiến người dùng thực thi các tác vụ theo mong muốn của kẻ tấn công).

Dấu hiệu lỗi CSRF:

- Nếu như ứng dụng chỉ dựa vào mỗi HTTP cookies thì ứng dụng đó có nguy cơ bị lỗi CSRF.

- Quan sát các chức năng cốt lỗi của ứng dụng và xác định các yêu cầu thực hiện đối với các dữ liệu nhạy cảm, nếu như mà kẻ tấn công có thể xác định được toàn bộ tham số đối với các yêu cầu (cho dù không thể xác định HTTP cookies) thì ứng dụng vẫn bị lỗi CSRF.

- Tạo ra trang HTML mà thực hiện những yêu cầu mong muốn mà không có sự tương tác về người dùng. Đối với các yêu cầu sử dụng GET thì có thể sử dụng thẻ <img> với tham số src=“chứa liên kết”. Nếu như những yêu cầu là POST có thể tạo ra những trường ẩn để chứa các tham số và có thể sử dụng Javascript để thực hiện tự động đệ trình form ngay sau khi trang được nạp.

* **Kiểm tra quản lý uỷ quyền**

*Kiểm tra lỗi Path traversal*

Sử dụng các thông tin thu thập được từ các bước kiểm tra trước, quan sát các kết quả thu thập được từ spider hoặc crawler để nhận biết, từ những kết quả mà spider mang lại chúng sẽ lần lượt kiểm tra các biến đối với các phương thức GET, POST hoặc COOKIE mà có khả năng bị lỗi. Hình thức kiểm tra này không cần sử dụng một công cụ nào mà chỉ đơn thuần thao tác các biến với ../ (dot-dot-slash) để truy cập đến file, thư mục, bao gồm cả source code, những file hệ thống. Tiến hành kiểm tra lại bằng cách sử dụng các thư viện của một số công cụ như Path Traversal Fuzz Strings, Appscan, Metasploit Pro.

*Kiểm tra lỗi Directory Traversal:*

- Quan sát các payload các payload liên quan đến Path Traversal đã gửi đến ứng dụng và nhận biết các dấu hiệu bất thường trong các phản hồi của ứng dụng.

- Trong quá trình tìm hiểu ứng dụng thì đối với kiểm tra các lỗi liên quan đến Path Traversal , nên chú trọng đến các chức năng đọc và ghi trên tập tin của ứng dụng.

- Nếu có các điểm liên quan đến đọc và ghi tập tin thì thử thao tác với các tập tin khác hoặc đường dẫn khác.

- Ứng dụng có 2 khả năng xảy ra khi thực hiện thay đổi nội dung tại các điểm liên quan đến đọc và ghi tập tin. Một có thể ứng dụng sẽ xứ lý tiếp hoặc là thông báo về việc sai đường dẫn trên ứng dụng. Nếu như quá trình đệ trình thất bại thì có thể thực hiện encode các payload và thử lại.

Nếu như ứng dụng có kiểm tra phần mở rộng của tập tin thì có thể thực hiện kiểm tra với các payload như cũ nhưng có thêm %00. Ví dụ: .../../../boot.ini%00.jpg

*Kiểm tra leo thang đặc quyền*

Trong giai đoạn này, các thử nghiệm cần xác minh rằng ứng dụng cho phép người dùng thay đổi đặc quyền của mình hay không, hoặc làm sao để có cách mà cho phép các cuộc tấn công leo thang đặc quyền. Quá trình kiểm tra gồm các bước:

- Kiểm tra role/privilege manipulation: Trong các thành phần ứng dụng, có phần cho phép người dùng tạo sửa xóa cơ sở dữ liệu (như profile, đơn hàng chẳng hạn). Kiểm tra xem có thể truy cập đến người dùng khác hay không, hoặc vai trò của người dùng khác mà người dùng này không có.

- Quá trình thao tác chủ yếu với HTTP request, bằng cách chính sửa yêu cầu của người dùng.

* **Kiểm tra các dữ liệu đầu vào**

Từ kết quả của quá trình điều tra ứng dụng, bước tiếp theo cho quá trình kiểm thử xâm nhập là việc quan sát các điểm nhập liệu đối với ứng dụng. Các điểm nhập dữ liệu thường là các tham số trên URL, các trường nhập liệu trong phần body, các trường cookie.......

*Kiểm tra lỗi XSS*

XSS là một trong những kĩ thuật tấn công phổ biến nhất hiện nay, đồng thời nó cũng là một trong những vấn đề bảo mật quan trọng đối với các nhà phát triển web và cả những người sử dụng web. Bất kì một website nào cho phép người sử dụng đăng thông tin mà không có sự kiểm tra chặt chẽ các đoạn mã nguy hiểm thì đều có thể tiềm ẩn các lỗi XSS. Thử nghiệm nhúng các đoạn mã (scrip) vào các form nhập liệu và các dữ liệu đầu vào trên trình duyệt để tìm ra lỗi XSS. Việc kiểm tra có thể sử dụng các công cụ chuyên biệt hoặc bằng tay chèn các chuỗi script vào đối tượng :

*“><script >alert(document.cookie)</script >*

*“><ScRiPt>alert(document.cookie)</ScRiPt>*

*“%3e%3cscript%3ealert(document.cookie)%3c/script%3e*

*“><scr<script>ipt>alert(document.cookie)</scr</script>ipt>*

*%00”><script>alert(document.cookie)</script>*

*Kiểm tra lỗi SQL injection*

Để kiểm tra lỗi SQL Injection, thực hiện tìm ra các tham số, input mà Web app truy vấn đến cơ sở dữ liệu. Từ đó nhúng những câu lệnh thích hợp vào các tham số đó để truy vấn đến cơ sở dữ liệu, và xem nó có khả năng thực thi được hay không. Lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lí bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase.

Để kiểm tra trang nào bị lỗi SQL Injection, chúng ta có thể thêm các ký tự sau trong tham số truyền vào của input:

Thường kết quả nhận đc là sẽ có thông báo lỗi. Nhưng nếu chỉ là 1 thông báo chung chung, chuyển hướng người dùng tới trang chủ hoặc refresh lại trang trước thì có thể là Blind SQL Injection.

Việc kiểm tra khả năng tấn công SQL injection:

- Trong quá trình gửi payload liên quan đến lỗi SQL Injection nếu như xuất hiện các phản hồi bất thường khi mà ứng dụng xử lý thì quan sát nguyên nhân gây ra lỗi từ tham số nào

- Nếu như có bất kỳ thông điệp lỗi database nào trả về thì quan sát về mặt nghĩa của câu thông báo (SQL Syntax và Error).

- Nếu như đệ trình các tham số với giá trị có kèm theo ‘ mà gây ra lỗi hoặc có phản hồi bất thường thì tiếp tục đệ trình lại tham số đó nhưng giá trị kèm theo hai dấu ‘, nếu như ứng dụng không xuất hiện lỗi thì có khả năng ứng dụng bị lỗi SQL Injection.

- Thử các hàm của SQL liên quan đến việc cộng chuỗi và đánh giá các phản hồi từ ứng dụng. Nếu như có kết quả giống với kết quả gốc (khi chưa chèn thêm các hàm cộng chuỗi) thì ứng dụng cũng có khả năng bị SQL Injection. (Lưu ý là phải encode nếu như sử dụng các ký tự đặc biệt)

- Nếu như dữ liệu của tham số là số thì hãy thử thực hiện với các biểu thức toán học đến tham số. Ví dụ nếu dữ liệu tham số là 2 thì hãy thử 3-1 hoặc 1+1, nếu như ứng dụng vẫn phản hồi giống như chưa thay đổi tham số thì ứng dụng có khả năng bị SQL Injection.

- Có thể thực hiện kiểm tra với dữ liệu là số bằng cách sử dụng các hàm liên quan đến chuỗi và số của SQL trong khi thực hiện đánh giá. Ví dụ dữ liệu vẫn là giá trị 2 thì có thể kiểm tra với payload 67-ASCII(‘A’) hoặc 51-ASCII(1)

- Kiểm tra các tham số có thể chèn thêm các hàm SQL mà liên quan đến thời gian chờ ví dụ như waitfor trong MSSQL hay là benchmark trong MySQL, sleep, … Nếu như các yêu cầu khi gửi đi với việc chèn trên mà có độ trễ thì có thể ứng dụng bị lỗi SQL Injection.

- Nếu như đã xác định được ứng dụng đã bị lỗi và xem thử khả năng khai thác lỗi đến đâu thì có thể dùng các công cụ như sqlmap,sqlninja, Haviji, … để đánh giá

*Kiểm tra lỗi LDAP injection*

LDAP là viết tắt của Lightweight Directory Access Protocol. LDAP là một giao thức để lưu trữ thông tin về người sử dụng, máy chủ, và các đối tượng khác. LDAP injection là tấn công nhằm vào máy chủ, mà từ đó tiết lộ nhiều thông tin nhạy cảm về người dùng, thậm chí có thể sửa đổi, chèn.

Nếu ứng dụng có lỗi LDAP injection, sẽ thu được toàn bộ thông tin về người dùng. Tuy nhiên điều này còn phụ thuộc vào quyền của tài khoản dùng để kết nối đến LDAP server. Có thể sử dụng các dấu '(', '|', '&', '\*' để bắt lỗi.

Xét một ứng dụng web có form search user như sau:

<input type="text" size=20 name="userName">Insert the username</input>

Và truy vấn LDAP như sau:

String ldapSearchQuery = "(cn=" + $userName + ")";

System.out.println(ldapSearchQuery);

Nếu như nhập “\*” vào box search thì hệ thống sẽ trả về tất cả các username có trong LDAP

*Kiểm tra lỗi XML injection*

Để kiểm tra XML injection, sử dụng các ký tự injection thông thường của XML vào các biến số (‘), < >, <![CDATA[ / ]]>,… trong các query.

*Kiểm tra lỗi Xpath injection*

Tương tự như SQL injection, Xpath injection xảy ra khi một trang web sự dụng thông tin người dùng cung cấp mà không kiểm soát để thực hiện một truy vấn Xpath cho dữ liệu XML. Bằng cách gửi đi thông tin đã bị thay đổi để thực hiện một truy vấn bât hợp pháp. Xpath là một ngôn ngữ tiêu chuẩn, có nghĩa là ký hiệu/ cú pháp của nó luôn thực hiện một cách độc lập, vì thế nên các cuộc tấn công có thể tự động hóa.

Để kiểm tra lỗ hổng XPath injection tương tự như SQL injection, sẽ thêm dấu (') để tạo ra truy vấn sai, rồi kiểm tra những thông tin thu được từ thông báo lỗi (error message).

*Kiểm tra lỗi IMAP/SMTP injection*

Mối đe dọa này ảnh hưởng tới các giao tiếp tới máy chủ mail (IMAP/SMTP), thường là webmail. Để kiểm tra IMAP/SMTP Injection, thực hiện kiểm tra xem có thể thêm các lệnh tùy ý vào các máy chủ mail, do các dữ liệu đầu vào không được lọc. Một số kiểu tấn công thường thấy là:

- Khai thác các lỗ hổng của giao thức IMAP/SMTP

- Lộ thông tin (Information leaks)

- Relay/SPAM

- Các bước tấn công là:

- Xác định các thông số dễ bị tổn thương

- Tìm hiểu về luồng dữ liệu và cơ cấu của khách hàng

- IMAP/SMTP command injection

*Kiểm tra lỗi command injection*

Tiến hành kiểm tra nếu nó có thể inject vào ứng dụng và dữ liệu sau đó được thực hiện bởi các máy chủ web. Tìm những URL có thể chứa các parameter cho phép thực thi lệnh như $cmd=, $command=... từ đó kẻ tấn công có thể thực thi được những code ảnh hưởng đến an toàn hệ thống.

*Việc kiểm tra lỗi Command injection :*

- Nếu như quá trình gửi payload liên quan đến việc kiểm tra OS Command Injection mà phía ứng dụng phản hồi có sự delay thì khả năng ứng dụng bị lỗi OS Command

- Injection, lặp lại kiểm tra với việc thay đổi payload để xác định liệu ứng dụng bị lỗi thực sự hay không.

- Thay thế payload ping command bằng các lệnh hệ thống khác như là ls, dir, để xác định có xuất hiện kết quả trên trình duyệt hay không

- Nếu ứng dụng bị lỗi OS Command Injectiont thì có thể sử dụng các công cụ khai thác để xem mức độ hệ thống bị ảnh hưởng bởi lỗi này.

*Kiểm tra lỗi tràn bộ đệm*

Lỗi tràn bộ đệm là lỗi khi mà tiến trình lưu trữ dữ liệu vượt ra ngoài vòng nhớ được cấp phát. Kết quả là dữ liệu có thể bị ghi đè lên vùng nhớ liền kề. Dữ liệu bị chèm có thể là bộ nhớ đệm khác, các biến và dữ liệu điều khiển chương trình (program flow control).Thực hiện kiểm tra lần lượt từng loại lỗ hổng tràn bộ đệm (buffer overflow) khác nhau, bao gồm:

- Heap overflow

- Stack overflow

- Format string

Heap overflow: Heap là một phân đoạn bộ nhớ được sử dụng để lưu trữ biến động, biến toàn cục. Mỗi đoạn bộ nhớ trong heap bao gồm thanh ghi ranh giới chứa thông tin quản lý bộ nhớ. Khi heap-based buffer overflow xảy ra, các thông tin kiểm soát bị ghi đè. Khi overflow được thực hiện một cách có kiểm soát, lỗ hổng sẽ cho phép kẻ tấn công ghi đè lên một vị trí bộ nhớ mong muốn một giá trị sử dụng điều khiển. Trong thực tế, một kẻ tấn công sẽ có thể ghi đè lên con trỏ chức năng và các địa chỉ khác nhau được lưu trữ.

Stack overflow: Stack overflows xảy ra khi dữ liệu kích thước biến được sao chép vào bộ đệm chiều dài cố định nằm trên ngăn xếp chương trình mà không kiểm tra độ dài. Lỗ hổng này sẽ cho phép thực thi mã tùy ý hoặc từ chối dịch vụ.

Format string: thường được sử dụng để làm hỏng một chương trình hay để thực thi mã có hại. Vấn đề bắt nguồn từ việc sử dụng của người dùng nhập vào không lọc các tham số chuỗi định dạng, như printf().

*Kiểm tra lỗ hổng tiềm tàng*

Sử dụng một số công cụ dạng proxy như XSS-proxy, hay Burp Suite để tiến hành kiểm tra các lỗ hổng kiểu incubated. Các bước kiểm tra được thực hiện thử nghiệm trong một vài dạng như sau:

- Cố gắng tải một tệp tin có chứa mã độc hoặc các mã (scrip) nguy hiểm đến người dùng và cố gắng công bố (public) tập tin đó để người dùng duyệt qua liên kết (url) tin cậy của website. Việc này nhằm mục đích lợi dụng website để lấy thông tin của người dùng.

- Thực hiện tấn công qua XSS (Không phát hiện ra khả năng các lỗ hổng dạng tiềm tàng được khai thác qua XSS)

- Thực hiện tấn công qua SQL/XPath Injection (Không phát hiện ra khả năng các lỗ hổng dạng incubated được khai thác qua SQL/XPath Injection)

* **Kiểm tra khả năng tấn công từ chối dịch vụ**

Về căn bản đều là việc tấn công dịch vụ rất nguy hiểm làm cho hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi 1 cách đáng kể với người dùng hợp lệ, bằng cách làm quá tải tài nguyên, băng thông của hệ thống. Tuy nhiên, loại lỗ hổng bảo mật ở mức ứng dụng có thể cho phép một người dùng độc hại để thực hiện chức năng nhất định, hoặc đôi khi, làm toàn bộ trang web không sẵn sàng. Những vấn đề này được gây ra bởi lỗi trong ứng dụng và thường được kích hoạt bởi đầu vào không mong muốn. Trong kiểm tra này chỉ tiến hành kiểm tra tấn công dựa trên một máy tính duy nhất.

*Kiểm tra truy vấn CSDL*

Tiến hành thực hiện nhiều kiểu truy vấn sử dụng nhiều ký tự đặc biệt và kết hợp với nhau để làm cho cơ sở dữ liệu phải thực hiện nhiều và liên tục các truy vấn, tìm kiếm có thể dẫn tới cạn kệt tài nguyên CPU. Thông thường thì các tổn thương này nằm trong chức năng tìm kiếm của website.

*Kiểm tra tràn bộ đệm*

Kiểm tra xem có thể từ chối dịch vụ bằng cách làm tràn một hoặc nhiều cấu trúc dữ liệu của ứng dụng. Kiểm tra xem nó có thể cạn kiệt tài nguyên máy chủ bằng cách làm cho nó phân bổ một số lượng rất lớn các đối tượng. Để kiểm tra, trước hết cần phải tìm cặp name/value. Sau đó, thiết lập một giá trị cực lớn, và xem máy chủ đáp ứng.

*Kiểm tra dữ liệu thành vòng lặp*

Tiến hành kiểm tra gửi các yêu cầu (request) kèm theo các giá trị khác nhau để tìm các biến có khả năng tạo vòng lặp có khả năng bị khai thác bằng cách thực hiện nhiều lần một tác vụ khiến tài nguyên hệ thống bị cạn kiệt.

*Kiểm tra lưu trữ dữ liệu từ người dùng lên hệ thống*

Bước đánh giá này thực hiện để xem xét khả năng người dùng có được phép sử dụng nhiều dữ liệu trên hệ thống hay không. Với lỗi này, thử nghiệm khả năng gửi nhiều dữ liệu lên hệ thống để kiểm tra xem hệ thống có kiểm tra các độ lớn của dữ liệu hay không. Và kiểm tra cơ chế ghi logfile của hệ thống.

*Kiểm tra lỗi trong quá trình thực hiện ngắt tài nguyên*

Bước đánh giá này được thực hiện để xem xét khả năng ứng dụng web có ngắt các tài nguyên đúng cách không sau khi chúng đã được sử dụng. Nếu một lỗi xuất hiện có khả năng ngăn chặn việc ngắt các tài nguyên sau khi đã sử dụng này thì có thể dẫn tới việc kẻ tấn công lợi dụng để tấn công DoS. Với lỗi này để xác định cần thực hiện kiểm thử hộp trắng.

*Kiểm tra lưu trữ dữ liệu trong mỗi phiên*

Bước đánh giá này được thực hiện để kiểm tra khả năng ứng dụng có lưu trữ một lượng lớn dữ liệu trong mỗi phiên của người dùng, đây là một trong những khả năng có thể gây ra DoS. Việc này có thể sẽ trở nên nguyêm trọng hơn nếu các phiên này được lưu trữ các thông tin đăng nhập theo định kỳ, việc này có thể giúp kẻ tấn công thực hiện tấn công DoS mà không nhất thiết cần tài khoản. Tuy nhiên để xác định được khả năng có thể xảy ra thì cần kiểm thử hộp trắng mới có thể xác định được.

* **Kiểm tra các dịch vụ Web**

*Kiểm tra ngôn ngữ định danh*

WSDigger là một công cụ miễn phí mã nguồn mở để tự động thử nghiệm web services. Với công cụ này, có thể thử nghiệm các web services, tương tác thông qua một giao diện đơn giản, nhập truy vấn tìm kiếm và gọi dịch vụ web tự động, mà không cần viết mã.

*Kiểm tra cấu trúc XML*

XML cần đúng cấu trúc để hoạt động đúng. Quá trình phân tích XML được thực hiện ở máy chủ, tiêu tốn rất nhiều tài nguyên, CPU. Một số kiểu tấn công bằng cách gửi lượng lớn tin nhắn XML hoặc XML sai cấu trúc. Việc kiểm tra có thể tạo ra các XML sai cấu trúc nhằm kiểm tra khả năng một cuộc tấn công từ chối dịch vụ, với mục tiêu làm tiêu tốn CPU và bộ nhớ.

*Kiểm tra HTTP GET parameters/REST*

Nhiều ứng dụng XML được gọi bằng cách đi qua các thông số bằng cách sử dụng HTTP GET. Đôi khi được gọi là “REST-style" Web Services (REST = Representational State Transfer). Web Services có thể bị tấn công bằng malicious content trong HTTP GET string như: extra long parameters, SQL injection, OS Injection. Để kiểm tra, tiến hành thay đổi các tham số, từ đó thực thi các cuộc tấn công. Có thể sử dụng WSDigger.

*Kiểm tra tấn công Naughty SOAP attachments*

Một ứng dụng web cho phép người dùng đính kèm các file dễ bị tấn công Naughty SOAP. Kiểu tấn công này dựa trên Web Services chấp nhận file đính kèm. Vấn đề nguy hiểm nằm trong việc xử lý các tập tin đính kèm trên máy chủ và phân phối lại các tập tin cho khách hàng.

*Kiểm tra tấn công Web Service replay*

Mối đe dọa của tấn công gửi lại (replay attack) là những kẻ tấn công có thể giả định danh tính của một người dùng hợp lệ và làm cho một số hành động bất chính mà không phát hiện. Để phát hiện, tiến hành theo các bước:

- Sử dụng Wireshark, nghe lén lưu thông mạng (sniff traffic)

- lọc các dữ liệu dịch vụ web (filter web service traffic).

Một lựa chọn khác là cài đặt WebScarab và sử dụng nó như một proxy để nắm bắt lượng truy cập http Sử dụng phần mềm thu thập gói tin (packets captured) như ethereal, TCPReplay để triển khai tấn công gửi lại (replay attack). Cũng có thể sử dụng ngay WebScarab để gửi lại (replay). Kết thúc quá trình này, nếu truy cập thành công có nghĩa là có thể tấn công gửi lại (replay).

* **Kiểm tra AJAX**

AJAX (tiếng Anh: "Asynchronous JavaScript and XML" - nghĩa là "JavaScript và XML không đồng bộ") là một nhóm các công nghệ phát triển web được sử dụng để tạo các ứng dụng web động hay các ứng dụng giàu tính Internet (rich Internet application).

Các ứng dụng AJAX có đầy đủ lỗ hổng bảo mật ứng dụng như web truyền thống. Lập trình không an toàn có thể dẫn đến SQL injection, không một yêu cầu chứng nhận phù hợp và ủy quyền có thể dẫn đến vấn đề bảo mật và tính toàn vẹn. Ngoài ra, các ứng dụng AJAX có thể được dễ bị tổn thương bởi biến thể tấn công của XSS: Cross Site Request Forgery (XSRF).

Đánh giá các ứng dụng AJAX có thể khó khăn hơn, bởi cách giao tiếp giữa máy trạm (client) và máy chủ (server). Trong các ứng dụng web truyền thống, tiêu chuẩn HTML hình thức gửi qua yêu cầu GET hoặc POST đã định dạng, và do đó dễ dàng để sửa đổi hoặc tạo ra các yêu cầu mới. Ứng dụng AJAX thường sử dụng mã hóa khác nhau, chương trình để gửi dữ liệu POST gây khó khăn cho công cụ kiểm tra.

## Các phương thức, giải pháp bảo vệ an toàn ứng dụng web

**Đánh giá bảo mật thường xuyên ứng dụng web**

Hầu hết các ứng dụng web đang hoạt động hiện này đều tiềm ẩn các mối đe dọa, cũng như các lỗ hổng, điểm yếu mà chưa được phát hiện để khắc phục, những lỗ hổng này có thể xuất phát từ sai sót trong cấu hình, hoặc từ việc phát triển ứng dụng cho phép tin tặc có thể khai thác. Thông qua việc đánh giá bảo mật ứng dụng, các chuyên gia sẽ sử dụng kinh nghiệm và kỹ năng lập trình công cụ để kiểm tra và khai thác các lỗ hổng bảo mật trên ứng dụng. Quá trình Kiểm tra bảo mật ứng dụng web sẽ giúp các tổ chức sớm phát hiện các lỗ hổng về an toàn thông tin trên các ứng dụng web từ đó có thể đưa ra các phương án, giải pháp khắc phục các lỗ hổng bảo mật đã phát hiện, trước khi một cuộc tấn công thực sự xảy ra,

**Triển khai tường lửa ứng dụng web**

Tường lửa ứng dụng web (Web Application Firewall – WAF) là một giải pháp nhằm bảo vệ cho ứng dụng web tránh khỏi các lỗi bảo mật đã trình bày ở trên. WAF là một thiết bị phần cứng hoặc phần mềm được cài lên máy chủ có chức năng theo dõi các thông tin được truyền qua giao thức http/https giữa trình duyệt của người dùng và máy chủ web tại lớp 7. Một WAF có khả năng thực thi các chính sách bảo mật dựa trên các dấu hiệu tấn công, các giao thức tiêu chuẩn và các lưu lượng truy cập ứng dụng web bất thường. Đây là điều mà các tường lửa mạng khác không làm được.

**Lập trình an toàn**

Hầu hết các lỗi hiện nay tồn tại trên ứng dụng web đều do các lập trình viên lúc phát triển ứng dụng không chú ý tuân thủ các tiêu chuẩn về lập trình an toàn, việc kiểm soát dữ liệu đầu vào cũng như dữ liệu đầu ra đang được thực hiện lỏng lẻo dẫn đến việc tồn tại các lỗ hổng như sql injection, xss, file upload..

Việc cung cấp cho đội ngũ phát triển ứng dụng các quy trình, hướng dẫn lập trình an toàn sẽ giúp giảm thiểu và ngăn chặn các cuộc tấn công do sai sót từ người lập trình gây ra.

## Các phương thức, giải pháp bảo vệ hệ thống thư điện tử

### 7.6.1. Sử dụng các công cụ phòng chống thư rác, thư giả mạo

Các công cụ phòng chống thư rác, thư giả mạo là thiết bị hoặc phần mềm có chức năng phát hiện, lọc và ngăn chặn các thư giả mạo được gửi đến hoặc gửi đi từ máy chủ thư điện tử. Đây là các công cụ không thể thiếu đối với các hệ thống thư điện tử trongcông tác phòng chống thư rác và thư giả mạo. Công cụ này cho phép “xóa” hoặc “đánh dấu là thư rác” các thư điện tử dựa trên các bộ luật (rule) do quản trị hệ thống thiết lập.

### 7.6.2. Thiết lập cấu hình cho công cụ phòng chống thư rác, thư giả mạo

Để hạn chế, ngăn chặn việc máy chủ thư điện tử nhận phải thư giả mạo, cần đặt cấu hình cho các công cụ phòng chống thư rác, thư giả mạo đáp ứng các yêu cầu sau đây:

- Đánh dấu thư rác đối với các thư điện tử gửi đến từ các địa chỉ IP nằm trong danh sách địa chỉ IP đen (Black List) do các tổ chức chống thư rác quốc tế có uy tín cung cấp (sbl.spamhaus.org, dnsbl.njabl.org, cbl.abuseat.org, bl.spamcop.net, dnsbl.sorbs.net v.v…).

- Đánh dấu thư rác với các thư điện tử có các bản ghi sau không hợp lệ: bản ghi MX; bản ghi PTR; bản ghi SPF; bản ghi DomainKeys Identified Mail (DKIM).  
- Đánh dấu thư rác với các thư điện tử có chứa các dấu hiệu đặc trưng thu được  
khi phân tích thư giả mạo, thư rác đã nhận được (ví dụ: tên hòm thư, địa chỉ máy chủ thư, đoạn ký tự đặc biệt v.v…). Tuy nhiên biện pháp này dễ dẫn đến khả năng chặn nhầm. Do đó khi lựa chọn biện pháp này thì cần xác định thật rõ các dấu hiệu đặc trưng, duy nhất có thể phân biệt thư giả mạo và thư khác.

### 7.6.3. Một số biện pháp quan trọng khác

*Cấu hình đầy đủ và chính xác các bản ghi (DNS) phân giải tên miền và địa chỉ IP của máy chủ thư điện tử*

Việc cấu hình đầy đủ các bản ghi DNS dưới đây không giúp máy chủ thư điện tử của cơ quan, tổ chức lọc được thư giả mạo gửi đến nhưng giúp cho các máy chủ thư điện tử khác có thể lọc được các thư điện tử giả mạo địa chỉ của chính cơ quan, tổ chức của ta. Khi cấu hình tên miền (DNS) cần chú ý các bản ghi sau đây:  
 + Bản ghi PTR: Đặt đúng giá trị tên miền của máy chủ thư điện tử. Việc này giúp  
phân giải địa chỉ IP ra tên miền được chính xác. Đồng thời hỗ trợ việc kiểm tra phân  
biệt thư hợp lệ và thư giả mạo được chính xác.

+ Bản ghi SPF: Đặt danh sách các địa chỉ IP được phép gửi thư theo tên miền của cơ quan, tổ chức. Người quản trị cần khai báo chính xác địa chỉ IP của máy chủ gửi thư điện tử để các hệ thống khác có thể loại trừ các địa chỉ IP gửi thư giả mạo địa chỉ của cơ quan. Cán bộ quản trị chú ý sử dụng tính năng "hard fail" ( "-all") để loại bỏ tất cả các máy chủ khác gửi thư dưới tên miền của cơ quan.

+ Bản ghi DKIM: Đặt khoá công khai của máy chủ thư điện tử do chức năng  
DKIM của máy chủ thư điện tử tạo ra. Chức năng này thường chỉ có ở các phiên bản mới phát hành của hệ thống thư điện tử, chức năng này cho phép kiểm tra chính xác nguồn gốc máy chủ gửi thư dựa trên việc ứng dụng giải thuật mã hóa công khai (mã hóa bất đối xứng)

Thường xuyên theo dõi, kiểm tra tên miền và địa chỉ IP của máy chủ thư điện tử trên danh sách đen (Blacklist) các tổ chức chống thư rác để đảm bảo tên miền và địa chỉ IP không bị đưa vào danh sách địa chỉ đen. Một số tổ chức cung cấp chức năng kiểm tra danh sách đen như: mxtoolsbox.com,spamhaus…

Nếu phát hi ện địa chỉ IP hoặc tên miền của máy chủ thư điện tử bị lọt vào danh sách đen thì người quản trị cần liên hệ với các tổ chức chống thư rác để tìm hiểu nguyên nhân, xử lý và tìm cách đưa tên miền hoặc địa chỉ IP của cơ quan, tổ chức ra khỏi danh sách này.

*Đào tạo kỹ năng và nâng cao nhận thức cho người dùng khi sử dụng thư điện tử, đặc biệt các vấn đề sau:.*

* Đặt và quản lý an toàn mật khẩu thư điện tử.
* Chỉ sử dụng các phương thức an toàn để truy cập hòm thư điện tử
* Phát hiện và báo cáo khi xuất hiện thư rác, thư giả mạo.

# Quản lý, đánh giá an toàn thông tin

## Nhu cầu và triển vọng đánh giá ATTT tại Việt nam

Việt nam đã có nhu cầu sử dụng sản phẩm CNTT từ cuối những năm 80 của thế kỷ 20. Không chỉ dừng lại trong việc sử dụng các sản phẩm CNTT nhập ngoại mà Việt nam còn phát triển một số sản phẩm an toàn phục vụ hoạt động ATTT nước nhà thuộc khu vực công. Trách nhiệm này thuộc về Ban cơ yếu chính phủ Việt nam.

Các sản phẩm CNTT có chức năng ATTT phải kể đến : (i) Các dịch vụ ATTT như Thư điện tử an toàn, Các ứng dụng liên lạc trực tuyến và phi trực tuyến an toàn, Hệ quản trị CSDL an toàn, Dịch vụ Web an toàn, Dịch vụ tiếng nói và truyền hình hội nghị trực tuyến, ... (ii) Các thiết bị cung cấp dịch vụ an toàn như điện thoại mật, thiết bị máy mã chuyên dụng, ... và (iii) Các cơ chế và hệ thống an toàn như Cơ chế quản lý và phân phối khoá bí mật, khoá công khai, dịch vụ chứng thực điện tử, hệ điều hành an toàn, bức tường lửa và mạng riêng ảo, ...

Cơ chế kiểm soát an toàn của các sản phẩm CNTT trên mới dừng lại chủ yếu ở việc đánh giá các mô đun mật mã bên trong các sản phẩm đó. Vấn đề đánh giá an toàn sản phẩm CNTT được tiến hành theo cách nhìn “Từng phần” mà chưa tiến hành theo cách vạn năng vì chúng ta chưa phát triển công tác đánh giá ATTT như các quốc gia phát triển khác.

Ngay đối với các mô đun mật mã tuy có truyền thống và kinh nghiệm lâu năm chúng ta cũng chưa làm được bài bản như FIPS 140 chẳng hạn. Đánh giá các mô đun mật mã dựa vào sự hiểu biết cao nhất có thể được về các thuật toán mật mã mà thiết kế các mô đun mật mã an toàn. Do đó chúng ta chưa thể nói được rằng công tác đánh giá các mô đun mật mã là hoàn toàn đầy đủ và toàn diện như đã được làm với FIPS 140.

Vấn đề đánh giá sản phẩm ATTT nói chung thì hoặc là theo cảm nhận hoặc theo cách thức “Từng phần” hoặc dựa vào những đánh giá chứng nhận cho sản phẩm đã nhập ngoại hoặc kiểm định những tấn công có thể được nói tới trong các tài liệu ATTT. Nói tóm lại chúng ta chưa có cơ chế sử dụng công cụ vạn năng để tiến hành đánh giá sản phẩm ATTT trong cả khâu sử dụng và phát triển sản phẩm ATTT.

Trong xu hướng phát triển đa dạng và phức tạp dần của các sản phẩm CNTT thì việc thiếu công cụ vạn năng đánh giá ATTT là một mối nguy cơ lớn vì chúng ta không thể kiểm soát được mức độ an toàn của sản phẩm CNTT ngay từ khâu thiết kế chế tạo và sử dụng triển khai.

Trong nhận thức của các bộ chuyên môn cơ yếu thậm chí các cán bộ nghiên cứu chuyên môn đầu ngành hoặc cho rằng đảm bảo được các mô đun mật mã an toàn trong các sản phẩm ATTT là đảm bảo được an toàn cho các sản phẩm đó hoặc nếu đề cập đến đánh giá kiểm định an toàn sản phẩm CNTT thì cũng chỉ với cách tiếp cận “Từng phần” mà thôi.

Rất nhiều cán bộ cho rằng đánh giá một sản phẩm ATTT của chúng ta là “đơn giản” vì mục tiêu chức năng của các sản phẩm ATTT của chúng ta “đơn giản”. Điều này cũng thật nguy hiểm vì rằng không có chức năng ATTT nào là đơn giản cả vì độ an toàn tổng thể của sản phẩm chỉ tương đương với độ an toàn của mắt xích yếu nhất về an toàn của sản phẩm đó.

Lại có ý kiến cho rằng sản phẩm của chúng ta không “vạn năng” như sản phẩm của nước ngoài và do đó cũng không cần cách tiếp cận “vạn năng” làm gì cho phức tạp. Đây cũng là điều cần chấn chỉnh vì rằng các phương pháp đánh giá không vạn năng không giúp chúng ta đánh giá được đầy đủ và tổng thể mức độ an toàn của một sản phẩm. Nó càng tỏ ra hạn chế một khi phân tích thiết kế và chế tạo sản phẩm mới hay khi phát hiện lỗ hổng an toàn thì cách khắc phục tổng thể và thiết kế chế tạo lại sẽ như thế nào.

Tựu chung ngay cả các chuyên gia mật mã đầu ngành vẫn chưa hình dung được sự khác biệt giữa vai trò của các mô đun mật mã trong sản phẩm ATTT với vai trò của cơ chế ATTT tổng thể của chính sản phẩm ATTT. Từ đó mà không thể đánh giá hết được tầm quan trọng của công tác đánh giá ATTT tổng thể đối với sản phẩm ATTT quan trọng như thế nào.

Nhiều cán bộ cơ yếu vẫn cho rằng đánh giá an toàn sản phẩm CNTT là tương đối đơn giản như đánh giá độ mật của các thuật toán mật mã - Điều mà chúng ta vẫn đang làm và đã có những thành tựu và kinh nghiệm đáng tự hào sau nhiều năm phát triển.

Coi nhẹ hoặc thấy khó khăn tốn kém trong công tác đánh giá ATTT có lẽ là hai khuynh hướng dễ thấy trong nhận thức của chúng ta. Coi nhẹ thì cho rằng không cần thiết vì tất cả mọi điều cốt lõi đều được cho rằng nằm trong khâu độ mật mật mã và chỉ chú tâm vào đánh giá mật mã mặc dù chúng ta vẫn sử dụng khai thác và phân tích thiết kế phát triển mới các sản phẩm ATTT.

Ngại khó khăn tốn kém cũng là một trở lực lớn. Nhiều người cho rằng Việt nam còn nghèo và lạc hâu và không phải là quốc gia lớn có tiềm lực mạnh thì không lên phát triển công tác đánh giá ATTT. Từ kinh nghiệm phát triển CNTT nói chung và đánh giá ATTT nói riêng thành công của Hàn quốc trong hơn 10 năm qua đáng để cho chúng ta suy nghĩ và học tập.

Chính vì vậy mà chúng ta không chỉ thúc đẩy tuyên truyền cho công tác đánh giá ATTT mà chúng ta còn phải định hướng và nâng cao nhận thức về công tác này ngay trong đội ngũ chuyên môn cao cấp của ngành.

Chúng ta thấy rằng xu thế hội nhập là không tránh khỏi và CNTT không phải là một ngoại lệ. Hơn nữa với dân số 82 triệu người và có một vị trí chiến lược trong khu vực đông nam châu Á với tiềm năng khoa học và công nghệ dồi dào, Việt nam không có cách nào khác là phải tự lực tự cường trong phát triển và sử dụng CNTT. Muốn vậy công tác đánh giá ATTT phải đặt ra cấp thiết hàng đầu.

Chúng ta không chỉ nhằm đánh giá lại những sản phẩm CNTT nhập ngoại mà còn phải đánh giá và thiết kế chế tạo an toàn những sản phẩm ATTT của chúng ta do thực tế đất nước đặt ra.

Khía cạnh tái đánh giá hoặc thừa nhận các chứng nhận đánh giá quốc tế các sản phẩm nhập ngoại sau khi có đủ năng lực chuyên môn để thẩm định những chứng nhận này là khía cạnh phổ biến. Không chỉ chúng ta mà các quốc gia khác cũng làm như vậy.

Khía cạnh thiết kế chế tạo và đánh giá sản phẩm ATTT đặc thù Việt nam đòi hỏi chúng ta phải tiến hành công tác đánh giá ATTT vạn năng. Bởi vì mức độ ATTT của các sản phẩm ATTT của chúng ta là sự đòi hỏi sống còn của khả năng độc lập tự chủ Việt nam. Trong vấn đề này chúng ta chỉ có một cách lựa chọn một khi chúng ta hội nhập khu vực và thế giới.

Do đó trong những năm tới Việt nam sẽ phát triển đánh giá trên 02 bình diện là : (i) Đánh giá kiểm định lại những sản phẩm CNTT nhập vào Việt nam để sử dụng. Đối với các sản phẩm này công tác đánh giá sẽ không đòi hỏi cấp thiết bằng công tác thẩm định chất lượng an toàn; (ii) Đánh giá thiết kế chế tạo và sử dụng sản phẩm ATTT mang nhãn hiệu Việt nam. Công tác đánh giá có thể phát triển mới hoặc mô phỏng các mô hình tiên tiến của cách tiếp cận vạn năng hiện nay.

Do đó Việt nam trong tương lai gần sẽ cần xây dựng 01 cơ quan thẩm quyền cấp chứng nhận và công nhận chứng nhận an toàn quốc tế của các sản phẩm CNTT và ít nhất 01 trung tâm đánh giá an toàn sản phẩm CNTT với hệ thống phòng thí nghiệm kiểm định với các phương tiện và công cụ đánh giá và đội ngũ cán bộ đánh giá đạt tiêu chuẩn quốc tế.

Trước mắt thì vấn đề luật pháp với ban hành luật làm hành lang pháp ly và các nghị định hướng dẫn thi hành luật là điều kiện tiên quyết cho hoạt động đánh giá ATTT tại Việt nam.

Hạ tầng cơ sở pháp lý chỉ ra nhà thẩm quyền xác tín, nhà thẩm quyền chứng nhận, nhà thẩm quyền đánh giá và sơ đồ chứng nhận và đánh giá an toàn CNTT quốc gia, chuẩn đánh giá an toàn CNTT và phương pháp luận đánh giá an toàn CNTT.

Sau khi đã có hạ tầng cơ sở pháp lý chúng ta mới chuyển sang xây dựng các phòng thí nghiệm kiểm định an toàn CNTT để tiến hành đánh giá an toàn CNTT.

Đi xa hơn nữa là việc ra nhập CCRA và hòa nhập quốc tế trong lĩnh vực đánh giá an toàn CNTT.

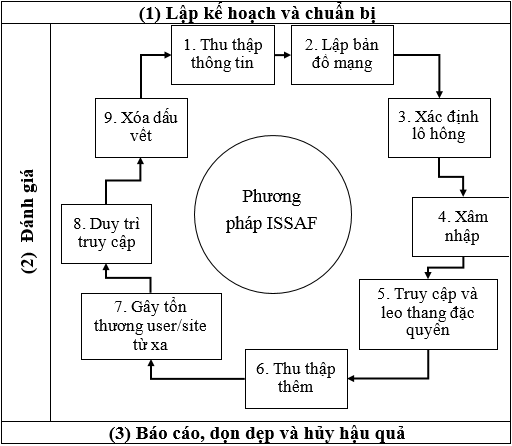
## Hệ thống tiêu chuẩn OWASP, ISSAF, OSSTMM

### 8.2.1. Phương pháp ISSAF

ISSAF là phương pháp đánh giá an toàn hệ thống thông tin của tổ chức OISSG, ra đời năm 2003. Khung làm việc của nó được phân vào một số loại lĩnh vực giải quyết các đánh giá an ninh theo một trình tự. Mỗi lĩnh vực đánh giá các bộ phận khác nhau của một hệ thống mục tiêu và cung cấp dữ liệu đầu vào cho nhóm công việc an ninh thành công. ISSAF phát triển tập trung vào hai lĩnh vực: quản lý và kỹ thuật. Mặt quản lý thực hiện quản lý nhóm công việc và các kinh nghiệm thực tế tốt nhất phải được tuân thủ trong suốt quá trình đánh giá, trong khi mặt kỹ thuật thực hiện bộ quy tắc cốt lõi, thủ tục cần tuân thủ và tạo ra một quy trình đánh giá an ninh đầy đủ.

Về mặt kỹ thuật, ISSAF xây dựng một loạt các phương pháp đánh giá cho từng thành phần của hệ thống CNTT như: đánh giá an toàn mật khẩu; đánh giá an toàn các thiết bị mạng: switch, router, firewall, IDS, VPN, anti-virus, SAN, WLAN…; đánh giá an ninh máy chủ: Windows, Linux, Novell, Web server; đánh giá an ninh ứng dụng web, mã nguồn, CSDL đến đánh giá an ninh phi công nghệ như an ninh vật lý; công nghệ xã hội.

Về phương thức làm việc, ISSAF bao gồm 3 giai đoạn tiếp cận và 9 bước đánh giá, đó là:



*Hình 8.1: Phương thức làm việc của ISSAF*

Giai đoạn 1: Lên kế hoạch và chuẩn bị

Đây là giai đoạn trao đổi thông tin ban đầu, lập kế hoạch và chuẩn bị cho đánh giá. Ký thỏa thuận đánh giá chính thức làm cơ sở pháp lý. Xác định thời gian và khoảng thời gian đánh giá, nhóm tham gia đánh giá, hướng leo thang…

Giai đoạn 2: Đánh giá

Đây là giai đoạn thực sự thực hiện đánh giá. Trong giai đoạn này, một cách tiếp cận theo lớp được tuân thủ. Có chín lớp đánh giá bao gồm:

- Lớp 1. Thu thập thông tin

- Lớp 2. Lập bản đồ mạng

- Lớp 3. Xác định lỗ hổng

- Lớp 4. Xâm nhập

- Lớp 5. Truy cập & leo thang đặc quyền

- Lớp 6. Liệt kê thêm

- Lớp 7. Thỏa hiệp user/site từ xa

- Lớp 8. Duy trì truy cập

- Lớp 9. Xóa dấu vết

Các bước được thực hiện lặp đi lặp lại đại diện bởi các mũi tên vòng tròn trong giai đoạn đánh giá trong hình 1.1. Đặc biệt chín lớp được mô tả rất kỹ và giới thiệu rất nhiều phần mềm tương ứng có thể sử dụng trong từng lớp hoặc tham khảo khi đánh giá.

Giai đoạn 3: Báo cáo, dọn dẹp và hủy hậu quả

Bao gồm báo cáo bằng lời nói (thực hiện khi có việc đột xuất hoặc vấn đề quan trọng khi đánh giá an toàn) và báo cáo cuối cùng thực hiện sau khi hoàn thành tất cả các bước đánh giá được xác định trong phạm vi công việc. Cuối cùng là dọn dẹp hậu quả, tất cả các thông tin được tạo ra hoặc được lưu trữ trên hệ thống đánh giá cần được loại bỏ khỏi hệ thống.

### 8.2.2. Phương pháp OWASP

OWASP ra đời năm 2001, đây là một tổ chức phi lợi nhuận, cộng đồng mở, mục tiêu chính của tổ chức là cải tiến an ninh các phần mềm ứng dụng, đặc biệt là ứng dụng web. Tổ chức này cũng xây dựng nhiều công cụ khác nhau cho việc đánh giá và đều là mã nguồn mở, miễn phí. OWASP ủng hộ phương pháp tiếp cận an ninh ứng dụng theo con người, quy trình và công nghệ vì đây là những nhân tố tạo ra phần mềm, những nhân tố trên có hành vi an toàn thì phần mềm an toàn. Theo OWASP, các ứng dụng web trên mạng hầu hết phải tiếp xúc với bên ngoài, nên nó sẽ là đối tượng đầu tiên chịu các cuộc tấn công phá hoại và sửa đổi trái phép. Vì vậy, đây sẽ là cánh cổng cho kẻ tấn công xâm nhập vào lớp ứng dụng trước khi thực hiện các bước tiếp theo xâm nhập vào hệ thống. Vì lỗ hổng an ninh này rất phổ biến, một số phương pháp đánh giá đã được giới thiệu nhằm đánh giá sự trầm trọng của các rủi ro an ninh cơ bản của ứng dụng web. Một nỗ lực được thực hiện bởi cộng đồng mở OWASP là xây dựng khung làm việc đánh giá an toàn ứng dụng web và thúc đẩy dự án OWASP top 10 nhằm nâng cao nhận thức an ninh ứng dụng của các tổ chức.

Dự án OWASP top 10 không tập trung vào các chương trình ứng dụng an ninh hoàn thiện, mà cung cấp một nền tảng cần thiết để tích hợp an ninh thông qua các nguyên tắc và thực hành lập trình an toàn. Dự án OWASP top 10 phân loại rủi ro an ninh ứng dụng web bằng cách đánh giá các hướng tấn công hàng đầu và lỗ hổng an ninh trong mối quan hệ đối với các tác động kỹ thuật và kinh doanh của nó. Việc đánh giá mười rủi ro hàng đầu của dự án sẽ thực hiện theo chu kỳ mỗi năm một lần nhằm mục đích chỉ ra những rủi ro nghiêm trọng nhất trong từng năm (chú ý không chỉ có 10 rủi ro cần xem xét mà rất nhiều, tuy nhiên hàng năm OWASP sẽ chọn ra 10 rủi ro nguy hại nhất).

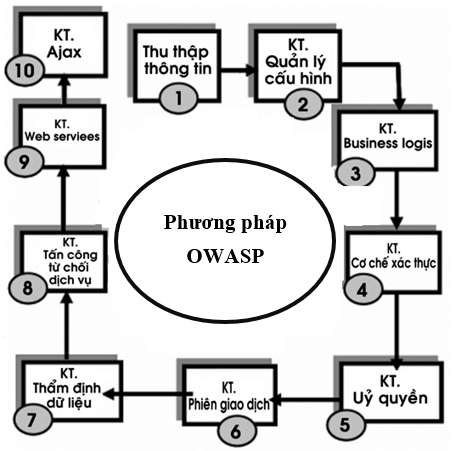
Dự án cũng cung cấp hướng dẫn cụ thể giúp đánh giá, xác minh và khắc phục từng phần các lỗ hổng của một ứng dụng như thế nào. Tuy không tập trung nhưng có một số hướng dẫn có sẵn từ cộng đồng OWASP cho những người phát triển và người đánh giá an toàn quản lý hiệu quả các ứng dụng web về mặt an ninh.

Đối với OWASP, an toàn phần mềm nói chung và ứng dụng web nói riêng phải được chú trọng ngay từ giai đoạn đầu tiên: định nghĩa, thiết kế và duy trì cho đến các giai đoạn sau này như: phát triển, triển khai, bảo trì. Tóm lại, đánh giá an toàn nên được áp dụng trong suốt vòng đời phát triển phần mềm. Vì vậy hướng dẫn này không chỉ dành cho người đánh giá mà còn phải được đọc và sử dụng bởi người phát triển và kiểm thử phần mềm. Giữ thông tin an ninh liên tục cập nhật là một khía cạnh quan trọng của dự án hướng dẫn này. Để đáp ứng yêu cầu trên, OWASP áp dụng phương pháp tiếp cận wiki, cộng đồng OWASP có thể phát triển và mở rộng thông tin trong tài liệu hướng dẫn này để bắt kịp với sự phát triển nhanh chóng của các mối đe dọa an ninh nhằm vào ứng dụng.

Theo OWASP, đánh giá an toàn sẽ không bao giờ là một khoa học chính xác với một danh sách đầy đủ của tất cả các vấn đề cần được đánh giá và đánh giá an toàn an ninh chỉ là một kỹ thuật thích hợp để đánh giá an tòa cho các ứng dụng web trong những hoàn cảnh nhất định. Phương pháp đánh giá an toàn ứng dụng web của OWASP dựa trên tiếp cận hộp đen. Người đánh giá không biết hoặc biết rất ít thông tin về các ứng dụng được đánh giá. Mô hình đánh giá bao gồm:

* Người đánh giá: thực hiện các hoạt động đánh giá.
* Công cụ và phương pháp: cốt lõi là dự án hướng dẫn đánh giá.
* Áp dụng: đánh giá hộp đen.

Phương pháp OWASP bao gồm 10 bước thực hiện chia thành 2 giai đoạn như sau:



Hình 8.2. Phương thức làm việc của OWASP

**Giai đoạn 1** – Chế độ thụ động: Trong chế độ này, người kiểm thử cố gắng hiểu được logic của ứng dụng và các thông tin liên quan đến mục tiêu kiểm thử. Các thông tin có thể thu thập được như: sơ đồ website, thông tin webserver, vị trí đặt tên miền, …. Các thông tin này là tiền đề để thực hiện giai đoạn thứ 2.

**Giai đoạn 2** – Chế độ chủ động: Trong giai đoạn này, người kiểm thử bắt đầu thực hiện kiểm thử theo hướng dẫn chi tiết trong tài liệu OWASP. OWASP chia tập kiểm thử chủ động thành 9 loại nhỏ với tổng số 66 bài viết hướng dẫn kiểm thử:

* Kiểm tra Quản lý cấu hình.
* Kiểm tra quản lý cấu hình
* Kiểm tra business logic
* Kiểm tra cơ chế xác thực
* Kiểm tra việc ủy quyền
* Kiểm tra quản lý phiên giao dịch
* Kiểm tra các dữ liệu đầu vào
* Kiểm tra khả năng tấn công từ chối dịch vụ
* Kiểm tra web services
* Kiểm tra AJAX

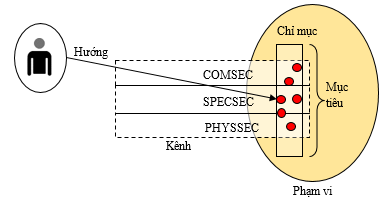
### 8.2.3. Phương pháp OSSTMM

OSSTMM là một dự án của Institute for Security and Open Methodologies (ISECOM) – tổ chức phi lợi nhuận được thành lập ở New York, Hoa Kỳ và ở Catalonia, Tây Ban Nha. Dự án này phát triển trong một cộng đồng mở, với các đối tượng tham gia bình đẳng và không ảnh hưởng bởi chính trị và thương mại. Đây là một phương pháp khoa học giúp mô tả chính xác các an ninh hoạt động (operational security – OpSec) đặc trưng thông qua đánh giá một cách nhất quán và lặp đi lặp lại trên các kênh vật lý, tương tác con người, kết nối như không dây, có dây, tương tự và số. Phương pháp này phù hợp với hầu hết các kiểu đánh giá như đánh giá an ninh, đánh giá lỗ hổng, … Hiện nay dự án được phát triển và nâng cấp lên tới phiên bản 3.0.

Từ góc độ kỹ thuật, phương pháp tiếp cận chia thành bốn nhóm chính, đó là phạm vi, kênh, chỉ mục và hướng. Phạm vi là tất cả các tài sản hoạt động trong môi trường mục tiêu trên đó xác định một quy trình thu thập thông tin. Một kênh xác định loại giao tiếp và tương tác với các tài sản có thể là vật lý, dải tầng số và truyền thông. Chỉ số là một phương pháp được coi là hữu ích khi phân loại và đếm các tài sản mục tiêu tương ứng với từng loại cụ thể của chúng, chẳng hạn như, địa chỉ MAC và địa chỉ IP. Cuối cùng, hướng mà theo đó người kiểm thử có thể đánh giá và phân tích từng tài sản chức năng. Toàn bộ quá trình này khởi tạo một lộ trình kỹ thuật theo hướng đánh giá toàn bộ môi trường mục tiêu và được gọi là phạm vi kiểm thử.

Phương pháp OSSTMM cũng định nghĩa một loạt các thuật ngữ được sử dụng như: kiểm soát, bề mặt tấn công, hướng, hướng tấn công, an ninh, an toàn, độ xốp, hạn chế, lỗ hổng, điểm yếu, RAV, hoạt động, an ninh hoàn hảo…

Ngoài ra, phương pháp OSSTMM xây dựng một cơ sở lý thuyết mô tả chi tiết các thành phần cấu thành an ninh hoạt động và lượng hóa các thành phần này cùng công thức tính toán của chúng. An ninh là một khái niệm tương đối mà với mức độ an ninh thực tế này thì có thể là tốt đối với tổ chức này nhưng lại quá mất an ninh so với tổ chức khác. Vì vậy, lượng hóa các thuộc tính an ninh giúp tính toán và biểu diễn an ninh một cách nhất quán và lặp đi lặp lại.

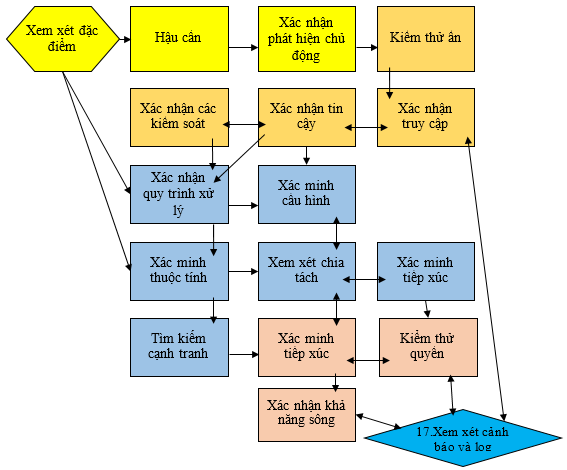


*Hình 8.3: Khái quát mô hình OSSTMM*

Phương pháp OSSTMM cũng định nghĩa một loạt các thuật ngữ được sử dụng như: kiểm soát, bề mặt tấn công, hướng, hướng tấn công, an ninh, an toàn, độ xốp, hạn chế, lỗ hổng, điểm yếu, RAV, hoạt động, an ninh hoàn hảo…

Ngoài ra, phương pháp OSSTMM xây dựng một cơ sở lý thuyết mô tả chi tiết các thành phần cấu thành an ninh hoạt động và lượng hóa các thành phần này cùng công thức tính toán của chúng. An ninh là một khái niệm tương đối mà với mức độ an ninh thực tế này thì có thể là tốt đối với tổ chức này nhưng lại quá mất an ninh so với tổ chức khác. Vì vậy, lượng hóa các thuộc tính an ninh giúp tính toán và biểu diễn an ninh một cách nhất quán và lặp đi lặp lại.

Phương thức làm việc của OSSTMM bao gồm 17 module kiểm thử như sau:



*Hình 8.4: Phương thức làm việc của OSSTMM*

Có năm kênh an ninh là: truyền thông, mạng dữ liệu, vật lý, con người và không dây chia thành 3 lớp kênh: COMSEC – truyền thông, mạng dữ liệu; SPECSEC – vật lý, con người; PHYSSEC – không dây. Ứng với mỗi kênh sẽ lần lượt thực hiện 17 mô-đun, chia thành 4 giai đoạn: giai đoạn bắt đầu gồm 3 mô-đun đầu tiên, giai đoạn tương tác gồm các mô-đun từ 4 đến 7, giai đoạn điều tra gồm các mô-đun từ 8 đến 13 và giai đoạn can thiệp gồm các mô-đun còn lại – từ 14 đến 17. Trong từng mô-đun, tùy thuộc vào từng kênh ta có các nhiệm vụ phải làm để có thể tìm được các giá trị cho 18 đại lượng ở phần trên (mô tả chi tiết trong chương 7, 8, 9, 10 và 11 của hướng dẫn OSSTMM). Như vậy, người kiểm thử phải thực hiện 17 \* 5 = 85 phân tích trước khi đưa ra được báo cáo cuối cùng.

## Thực hiện kiểm định, đánh giá hệ thống ATTT

Thực hiện kiểm định an toàn thông tin cho một cơ quan, tổ chức là công việc không dễ dàng và cần tuân theo một quy trình nhất định. Quy trình kiểm định phải đảm bảo phù hợp, đầy đủ và các kết quả kiểm định phải so sánh được với các yêu cầu đặt ra. Dưới đây là cụ thể về quy trình kiểm định áp dụng từ giai đoạn khởi tạo dự án cho đến khi kết thúc:



Hình 8.5: Quy trình kiểm định an toàn hệ thống thông tin

Bước 1: Thực hiện tại thời điểm bắt đầu kiểm định, các bên liên quan cần thống nhất các điều khoản chung và ký kết các thỏa thuận liên quan chuẩn bị cho quá trình kiểm định.

Bước 2: Dựa trên thỏa thuận giữa các bên, nhóm kiểm định sẽ lên một kế hoạch chi tiết các công việc cần thực hiện trong toàn bộ quá trình kiểm định.

Bước 3: Nhóm kiểm định tiến hành kiểm tra, xem xét các tài liệu có sẵn của bên kiểm định về việc thực hiện an toàn hệ thống thông tin. Nếu cần thiết có thể yêu cầu bổ sung tài liệu.

Bước 4: Thực hiện kiểm định trực tiếp thông qua một cuộc họp mở với những người tham gia là phụ trách các bộ phận liên quan của cơ quan, tổ chức để hỏi, phỏng vấn đề đảm bảo an toàn thông tin.

Bước 5: Thông tin thu được trong quá trình kiểm tra trực tiếp được củng cố thêm và đánh giá bởi đội ngũ kiểm định

Bước 6: Các kết quả kiểm toán được tóm tắt trong báo cáo kiểm định. Báo cáo này được cung cấp cho cơ quan có thẩm quyền xem xét cấp chứng nhận.

### 8.3.1. Chuẩn bị kiểm định

Khi có kế hoạch thực hiện một cuộc kiểm định, người quản lý của tổ chức được kiểm định phải tham gia. Trong giai đoạn này, cần quy định các đối tượng kiểm định, ký kết hợp đồng và thỏa thuận các điều khoản cần cho quá trình kiểm định (ví dụ cho phép xem các tài liệu).

Quản lý của tổ chức nên thông báo cho các cán bộ phụ trách, nhân viên về kế hoạch kiểm định. Các cán bộ phụ trách nên giải thích và nhắc nhở nhân viên phối hợp thực hiện kiểm định, đồng thời chuẩn bị hồ sơ tài liệu phục vụ cho các cán bộ kiểm định. Các tài liệu sau đây cần cung cấp cho nhóm kiểm định:

Tài liệu tổ chức

* Sơ đồ tổ chức hệ thống thông tin
* Các bộ phận thực hiện đảm bảo an toàn thông tin
* Lịch trình và kế hoạch thực hiện an toàn thông tin của tổ chức

Tài liệu kỹ thuật

* Các phân vùng mạng
* Vấn đề áp dụng các biện pháp đảm bảo an toàn
* Chính sách an toàn
* Danh sách các nguy cơ an toàn trong vòng 6 tháng
* Việc khắc phục, xử lý các nguy cơ

### 8.3.2. Tạo kế hoạch kiểm định

Khi đã có một cái nhìn đầy đủ về hệ thống thông tin của mục tiêu kiểm định và xác định được phạm vi kiểm định, nhóm kiểm định cần xây dựng một kế hoạch kiểm định. Kế hoạch này là công cụ chính được sử dụng trong suốt toàn bộ kiểm toán, và là tài liệu xác định tất cả các hoạt động kiểm định.

Việc phân bố thời gian trong quá trình thực hiện cũng rất quan trọng. Các nhiệm vụ cần thực hiện lâu phải được bố trí nhiều thời gian hơn, các nhiệm vụ đơn giản sẽ chỉ tốn ít thời gian. Phân bố thời gian sao cho toàn bộ các công việc có thể giải quyết được từ khi bắt đầu đến lúc kết thúc. Dưới đây là bảng thời gian ước tính khi thực hiện các giai đoạn kiểm định chung:

|  |  |  |
| --- | --- | --- |
| **Giai đoạn** | **Công việc** | **Thời gian (%)** |
| Bước 1 | Chuẩn bị kiểm định | 5% |
| Bước 2 | Tạo kế hoạch kiểm định | 15% |
| Bước 3 | Xem xét tài liệu | 20% |
| Bước 4 | Kiểm tra trực tiếp | 35% |
| Bước 5 | Đánh giá kết quả | 5% |
| Bước 6 | Lập báo cáo kiểm định | 20% |

Trong từng bước lại có các nhiệm vụ cụ thể. Thời gian thực hiện với các nhiệm vụ cụ thể phải được xem xét phù hợp với khoảng thời gan chung của toàn bộ giai đoạn.

### 8.3.3. Xem xét tài liệu

Sau khi đã có được các tài liệu cung cấp từ bước 1, bây giờ là lúc xem xét tài liệu để có cái nhìn tổng quan về toàn bộ hệ thống kiểm định. Khi xem xét tài liệu, cần kiểm tra các chính sách đã áp dụng với hệ thống mạng và các rủi ro xảy đến trong thời gian gần.

Xác định một chính sách phải đặt trong đặc điểm của các công ty, tổ chức, vị trí của nó, tài sản, công nghệ. Các chính sách phải được tính tới những vấn đề liên quan đến pháp lý và quy định các yêu cầu, hợp đồng hoặc nghĩa vụ của bên thứ 3 và bên phụ thuộc. Quản lý phải phê duyệt chính sách, và tất cả các nhân viên nên biết các chính sách, hiểu tầm quan trọng, mục đích của nó. Chính sách này phải bao gồm một khuôn khổ cho việc thiết lập các đối tượng, đưa ra hướng quản lý và hành động, thiết lập các tình huống quản lý rủi ro và đưa ra biện pháp chống lại những nguy cơ đã được tính tới. Chính sách có thể được xem như là một tập cha của chính sách an toàn thông tin, ví dụ như các chính sách đưa ra những vấn đề mà chính sách an toàn thông tin không cần thiết phải đề cấp tới.

Xác định rủi ro đối với tài sản có tính tới các mối đe dọa và điểm yếuliên quan tới tài sản này và những tác động làm mất đi tính bí mật, toàn vẹn, sẵn có của tài sản. Việc xác định tài sản, mối đe dọa, các lỗ hổng cần phải liên quan đến việc kiểm soát ở các khu vực khác nhau. Điều này là rất quan trọng để đảm bảo rằng tất cả tài sản đều được xác định vì đây là cơ sở để đánh giá rủi ro, và chủ sở hữu được xác định cho mỗi tài sản. Việc xác định những tác động làm mất tính bảo mật, toàn vẹn và sẵn sàng của tài sản nên tính đến những nguy hiểm mà công ty phải đối mặt như về luật pháp, quy định, hợp đồng và yêu cầu của công ty thông qua những thiệt hại đó. Phân tích và đánh giá các rủi ro dựa trên những thông tinbao gồm tất cả những khu vực điểu khiển như: tổ chức, nhân sự, quy trình kinh doanh, điều hành và duy trì, pháp lý, quy định và các vấn đề về hợp đồng, cơ sở xử lý thông tin. Điều này sẽ liên quan đến việc tổ chức đánh giá kết quả của việc kinh doanh từ những lỗi an toàn, có tính đến hậu quả mất tính bí mật, tính toàn vẹn, tính sẵn sàng của các tài sản có thể có. Điều này cũng bao gồm khả năng đánh giá các lỗi khi xảy ra, xem xét các mối đe dọa, điểm yếu được xác định và khả năng xảy đến cùng nhau và gây ra sự cố.

Khi tổ chức đã xác định, đánh giá và hiểu những tác động của rủi ro có thể có trong kinh doanh thì họ sẽ có những hành động khác nhau để quản lý hay khắc phục những rủi ro đó ở tình hình kinh doanh của họ. Những hành động của tổ chức có thể xem xét bao gồm việc áp dụng kiểm soát thích hợp giảm thiểu rủi ro, tránh những rủi ro không thông qua cam kết của một họat động rủi ro có liên quan, chuyển giao các rủi ro (toàn bộ hoặc một phần) cho một bên khác ví dụ như là doanh nghiệp bảo hiểm hay cố ý hoặc khách quan chấp nhận rủi ro. Những tùy chọn này hoặc kết hợp một số các tuỳ chọn khác của tổ chức, các tổ chức khác nhau với cùng một rủi ro nhưng lại có những kết luận khác nhau, điều này còn phụ thuộc vào đối tượng kinh doanh và tùy từng trường hợp. Trong bất cứ trường hợp nào điều quan trọng vẫn là xác nhận rằng các quyết định này được ghi chép tốt và tổ chức có thể cung cấp bằng chứng để quyết định này được thực hiện với đầy đủ kiến thức về rủi ro và không đơn giản chỉ là sự thiếu hiểu biết.

### 8.3.4. Kiểm tra trực tiếp

Mục đích của việc kiểm tra trực tiếp là để so sánh và kiểm tra lại các tài liệu được cung cấp với các điều kiện thực tế để xem vấn đề đảm bảo an toàn thực tế của tổ chức có đáp ứng đúng và đầy đủ như trong tài liệu hay không. Đôi khi quá trình lập kế hoạch rất hoàn hảo nhưng khi áp dụng lại phát sinh nhiều vấn đề, không được như mong muốn ban đầu.

Kiểm tra trực tiếp có thể được thực hiện theo nhiều cách khác nhau. Có thể là tổ chức một vài cuộc gặp mặt trực tiếp, với sự tham gia của tất cả các đối tượng liên quan; cũng có thể là gặp riêng từng đối tượng để xem xét theo từng khía cạnh.

Một vấn đề cần được quan tâm khi thực hiện kiểm tra là “kỹ thuật kiểm tra”. Kỹ thuật kiểm tra được hiểu là tất cả các phương pháp được sử dụng để xác định sự thật của vấn đề. Các kỹ thuật kiểm tra khác nhau sau đây có thể được sử dụng trong quá trình kiểm tra trực tiếp:

* Hỏi trực tiếp bằng lời (phỏng vấn)
* Kiểm tra bằng mắt của hệ thống, địa điểm, không gian, phòng, và các đối tượng
* Quan sát (ví dụ như quan sát ngẫu nhiên một phòng làm việc)
* Phân tích các tập tin (bao gồm cả dữ liệu điện tử)
* Kiểm tra kỹ thuật (ví dụ như thử nghiệm các hệ thống báo động, hệ thống kiểm soát truy cập, ứng dụng, …)
* Phân tích dữ liệu (ví dụ như các tập tin đăng nhập, đánh giá cơ sở dữ liệu, …)
* Đưa ra các câu hỏi bằng văn bản.

Tùy từng trường hợp cụ thể áp dụng các kỹ thuật kiểm định khác nhau, quan trọng là kết quả phải khách quan và có thể đánh giá được toàn bộ các khía cạnh cần thực hiện kiểm tra.

Để chứng thực, các bộ phận liên quan cần đưa ra bằng chứng cho người kiểm định. Những bằng chứng phải chứng minh được tổ chức đã tham gia một cách có tiếp cận hệ thống từ việc xác định phạm vi qua việc thực thi một hệ thống của các quy trình quản lý và các kiểm soát phù hợp với an toàn thông tin cần thiết cho việc kinh doanh. Cách tiếp cận cũng cần được chứng minh và thể hiện thông qua các quyết định quản lý phù hợp đã đưa ra việc làm thế nào để thỏa thuận với các mặt của rủi ro dựa trên việc lập trình các quy trình quản lý rủi ro. Ngoài ra có thể cung cấp các bằng chứng về các thủ tục đã được đưa ra để theo dõi, xem xét và áp dụng quy trình. Nhóm kiểm định sẽ dựa trên các thông tin được chứng minh để xem xét tính chính xác của thông tin và đưa ra các kết quả phù hợp.

### 8.3.5. Đánh giá kết quả

Sau khi kiểm tra trực tiếp, các thông tin thu được cần được đưa ra đánh giá. Việc đánh giá cũng có thể được thực hiện bởi nhóm kiểm toán hoặc các cơ quan có thẩm quyền. Các kết quả đánh giá sẽ là cơ sở chứng nhận tính an toàn của mục tiêu đánh giá và là điều kiện cấp chứng nhận đảm bảo an toàn thông tin.

Khi đánh giá kết quả, cần xem xét mục tiêu ban đầu để xác định ranh giới rủi ro và các rủi ro có thể chấp nhận được. Bất kỳ một loại trừ nào được tìm thấy do kiểm soát quản lý là rất cần thiết để đáp ứng các tiêu chuẩn chấp nhận rủi ro phải được chứng minh bằng các chứng cứ phù hợp mà các hành động được đưa ra bằng việc quản lý không bị ảnh hưởng tới tổ chức. Sự phù hợp với trách nhiệm quản lý rủi ro an toàn thông tin của nó và bất kỳ rủi ro nào được biết đến, được chấp nhận một cách khách quan bởi những người quản lý có trách nhiệm điều hành việc thực thi những quyết định đó và những người chịu trách nhiệm về việc ra quyết định như vậy.

### 8.3.6. Lập báo cáo kiểm định

Công việc cuối cùng trong kiểm định an toàn hệ thống thông tin là lập báo cáo các công việc và kết quả kiểm định. Báo cáo này trình bày chi tiết các thông tin chung về tài nguyên kiểm định, danh mục các mục kiểm định và kết quả kiểm định.

## Đánh giá mức độ rủi ro thông qua kiểm định

### 8.4.1. Các rủi ro xác định thông qua đánh giá

Sau khi thực hiện đánh giá, chúng ta có thể thu được thông tin về các rủi ro có thể xảy đến đối với hệ thống đánh giá. Các rủi ro được tìm thấy thông qua quá trình thực hiện đánh giá an toàn hệ điều hành, đánh giá an toàn webserver, đánh giá an toàn cơ sở dữ liệu, đánh giá an toàn ứng dụng web, đánh giá an toàn các thiết bị mạng và mạng không dây, … hoặc ngay trong quá trình dò quét thu thập thông tin ban đầu. Tùy từng hệ thống đánh giá mà chúng ta sẽ có được các kết quả khác nhau. Các kết quả thu được phụ thuộc vào hệ thống tồn tại nhiều hoặc ít điểm yếu, và khả năng khai thác các điểm yếu đó như thế nào.

Chúng ta cần tổng hợp thông tin từ tất cả các bước của quá trình thực hiện đánh giá, và sắp xếp theo các danh mục khác nhau để tiện cho việc lập báo cáo sau này. Ví dụ:

1. Các rủi ro tìm thấy trong quá trình thu thập thông tin
2. Các rủi ro tìm thấy khi thực hiện đánh giá an toàn hệ điều hành Windows:
3. Thông tin rủi ro
4. Mức độ nguy hiểm
5. Cách thức phát hiện
6. Các ảnh hưởng, ….
7. Các rủi ro tìm thấy khi thực hiện đánh giá an toàn hệ điều hành Linux
8. Các rủi ro tìm thấy khi thực hiện đánh giá an toàn cho WebServer
9. ….

### 8.4.2. Các rủi ro xác định thông qua kiểm định

Tương tự như đối với đánh giá an toàn hệ thống thông tin, sau khi thực hiện kiểm định an toàn cho một hệ thống thông tin, chúng ta cũng có thể xác định được các rủi ro có thể xảy đến với hệ thống kiểm định. Bây giờ chúng ta cần liệt kê chi tiết toàn bộ các rủi ro và sắp xếp theo một khuôn khổ nhất định để phục vụ cho quá trình lập báo cáo kiểm định sau này.

Thông thường, các rủi ro xác định thông qua kiểm định sẽ không nhiều bằng các rủi ro thu được qua quá trình thực hiện đánh giá. Bởi vì thường chúng ta chỉ thực hiện kiểm định trên một phạm vi hẹp, như: hệ thống máy chủ, hệ thống cơ sở dữ liệu, vấn đề thực thi chính sách, … chứ không kiểm định toàn bộ hệ thống. Như vậy các rủi ro sẽ được khoanh vùng trong phạm vi đánh giá chứ không phải rủi ro của cả hệ thống.

### 8.4.3. Phân loại rủi ro

Phân loại rủi ro cũng là một công việc rất cần thiết đối với người đánh giá và kiểm định. Việc phân loại rủi ro sẽ giúp cho bản báo cáo được cụ thể và rõ ràng hơn. Như thế ngay cả những người không hiểu biết nhiều về công nghệ thông tin hoặc không am hiểu về các tấn công cũng có thể dễ dàng xác định được các nguy cơ có thể xảy đến đối với hệ thống.

Tùy từng trường hợp và phân thành các mức độ rủi ro khác nhau. Tuy nhiên thông thường các rủi ro được chia làm 3 loại như sau:

* + - Rủi ro mức cao:

Đây là các rủi ro có mức ảnh hưởng nghiêm trọng tới hệ thống, và cho phép kẻ tấn công có thể chiếm quyền điều khiển hệ thống. Thông thường trong các chương trình đánh giá tự động, các rủi ro mức cao sẽ được thể hiện ở màu đỏ.

* + - Rủi ro mức trung bình:

Đây là các rủi ro có ảnh hưởng tới hệ thống nhưng không ảnh hưởng trực tiếp như các rủi ro ở mức cao. Các rủi ro ở mức trung bình thường là các rủi ro liên quan đến quyền sử dụng của người dùng bình thường, có thể thực hiện một số thao tác lên hệ thống nhưng không thể thực hiện các hành động của người quản trị. Tuy nhiên kẻ tấn công có thể lợi dụng các rủi ro này để tấn công leo thang đặc quyền, từ người dùng bình thường nâng quyền lên mức quản trị để chiếm quyền điều khiển hệ thống. Thông thường trong các chương trình đánh giá tự động, các rủi ro mức trung bình sẽ được thể hiện ở màu vàng.

* + - Rủi ro mức thấp:

Đây là các rủi ro có ảnh hưởng tới hệ thống nhưng ảnh hưởng ở mức thấp. Các rủi ro này thường là các rủi ro về lộ thông tin, lộ tài khoản email, hoặc sử dụng các thư mục ẩn trong hệ thống, … Khi bị khai thác, kẻ tấn công có thể biết được một vài thông tin liên quan trong hệ thống nhưng không thể chiếm quyền điều khiển hệ thống. Thông thường trong các chương trình đánh giá tự động, các rủi ro mức thấp sẽ được thể hiện ở màu xanh nhạt.