ĐẢM BẢO ATTT

Phần 1: Lý thuyết đảm bảo an toàn thông tin

**1. Tại sao vấn đề bảo mật thông tin lại là vấn đề quản lý?**

**2. Việc triển khai công nghệ mạng có tạo ra ít hoặc nhiều rủi ro cho doanh nghiệp sử dụng công nghệ thông tin? Tại sao?**

Việc triển khai công nghệ mạng có thể tạo ra rủi ro cho doanh nghiệp sử dụng công nghệ thông tin. Một hệ thống được kết nối đến internet, đồng nghĩa với việc tin tặc có khả năng truy cập trái phép qua mạng.

**3. Tống tiền thông tin là gì? Mô tả cách tấn công như thế có thể gây ra tổn thất, nêu ví dụ.**

‘Tống tiền thông tin’ là từ ghép giữa ‘tống tiền’ và ‘thông tin’. Đầu tiên, tin tặc sẽ làm lây lan phần mềm độc hại vào máy của nạn nhân, sau đó mã hóa các dữ liệu trên máy nạn nhân và đòi tiền chuộc để giải mã các văn bản đó. Thậm chí, khi có tiền chuộc rồi, thì tỷ lệ để lấy lại dữ liệu không phải là 100%. Cách tấn công này có thể gây tổn thất rất lớn, nếu dữ liệu bị mã hóa là những thông tin quan trọng của công ty, tổ chức (thông tin liên lạc với khách hàng, đối tác, v.v.). Nổi tiếng gần đây nhất là virus Wanna Cry, thông qua các lỗ hổng bảo mật của hệ điều hành Windows để lây lan chính bản thân nó. Theo một ước tính không chính thức, Wanna Cry gây thiệt hại khoảng 4 tỷ đô-la Mỹ cho những hoạt động của nó.

**4. Tại sao nhân viên lại là một trong những mối đe dọa lớn nhất với an ninh thông tin?**

Nhân viên của công ty là những người có đe dọa lớn nhất với an ninh thông tin, bởi họ là những người tiếp xúc trực tiếp và gần gũi nhất với thông tin, tài liệu, và không phải ai cũng giỏi và có hiểu biết về an ninh thông tin để phòng tránh các rủi ro có thể xảy ra. Khắc phục việc này có thể đưa ra cơ chế phân quyền, kiểm soát chặt chẽ, kỹ lưỡng.

**5. Nhận thức về hacker đã thay đổi như thế nào trong những năm gần đây? Hồ sơ của một hacker gồm những gì?**

Trước kia, hacker thường là nam giới, tuổi từ 13 đến 18, không được bố mẹ quan tâm và dành tất cả thời gian rảnh vào máy tính, trong khi hiện nay, một hacker có thể là nam hoặc nữ, từ 12 đến 60 tuổi với trình độ kỹ năng đa dạng, là người thuộc hoặc không thuộc một tổ chức nhất định.

**6. Sự khác biệt giữa một hacker có kỹ năng và một hacker không có kỹ năng (ngoài các cấp độ kỹ năng) là gì?**

Một hacker có kỹ năng thường là người có hiểu biết về giao thức mạng, thông thạo nhiều ngôn ngữ lập trình, biết cách khai thác các lỗ hổng của hệ thống mà mình định tấn công. Hacker có kỹ năng sẽ hiểu về hệ thống đủ sâu để viết ra các phần mềm tấn công và công bố trên mạng.

Hacker không có kỹ năng (script kiddies, packet money) là những người sử dụng phần mềm mà hacker có kỹ năng đã đăng tải mà không thực sự hiểu cách hoạt động của các phần mềm đó.

**7. Các loại phần mềm độc hại khác nhau như nào? Trojan horses khác virus và worm ở điểm nào?**

Phần mềm độc hại, là các chương trình làm hỏng, phá hủy hoặc từ chối dịch vụ của hệ thống đích. Ba loại phần mềm độc hại phổ biến nhất là: virus, worm, và trojan horse.

Virus tự gắn nó vào các một tệp hoặc ứng dụng có thể chạy được để lây lan. Worm thì tự sao chép và gửi chính nó đi. Trojan horse thì ẩn dưới dạng dữ liệu hoặc một chương trình vô hại.

**8. Nêu sự liên quan giữa các nhóm chính sách, tiêu chuẩn, chỉ dẫn. Cho một ví dụ về sự liên quan đó.**

Chính sách là luật của tổ chức. Tiêu chuẩn là yêu cầu bắt buộc để hỗ trợ các chính sách riêng lẻ. Chỉ dẫn là chi tiết từng hành động.

Ví dụ:

**9. Mục tiêu của an toàn bảo mật thông tin. Đưa ra ví dụ việc đảm bảo các mục tiêu của an toàn và bảo mật thông tin.**

- Mục tiêu của an toàn bảo mật thông tin: Bảo vệ tài nguyên của tổ chức, đảm bảo thực hiện tốt nhất nhiệm vụ. 3 mục tiêu chính

Availabillity: Tính sẵn sàng

Đáp ứng khi có yêu cầu, tuy nhiên thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn => thảm họa tấn công từ bên ngoài.

Integrity: Tính toàn vẹn

Cung cấp đúng thông tin, cung cấp thông tin chính xác.

Confidentiality: Tính cẩn mật (tin cậy)

Đảm bảo tính bí mật của thông tin. Thông tin chỉ được truy cập bởi người được phép.

- Đưa ra các ví dụ việc đảm bảo các mục tiêu của an toàn và bảo mật thông tin:

+ Availabillity: Máy của hacker sẽ gửi hàng loạt các gói tin có các MAC nguồn giả tạo đến switch làm bộ nhớ lưu trữ MAC address table của switch nhanh chóng bị đầy khiến switch không thể hoạt động bình thường được nữa. Đây cũng thuộc hình thức tấn công từ chối dịch vụ (DoS). Để tăng khả năng chống trọi với các cuộc tấn công cũng như duy trì độ sẵn sàng của hệ thống ta có thể áp dụng một số kỹ thuật như: Load Balancing, Clustering, Redudancy, Failover…

+ Integrity: Giải pháp “data integrity” có thể bao gồm thêm việc xác thực nguồn gốc của thông tin này (thuộc sở hữu của đối tượng nào) để đảm bảo thông tin đến từ một nguồn đáng tin cậy và ta gọi đó là tính “authenticity” của thông tin.

+ Confidentiality: Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập về cả mặt vật lý, ví dụ như tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó hoặc logic, ví dụ như truy cập thông tin đó từ xa qua môi trường mạng. Sau đây là một số cách thức như vậy:

• Khóa kín và niêm phong thiết bị.

• Yêu cầu đối tượng cung cấp credential, ví dụ, cặp username + password hay đặc điểm về sinh trắc để xác thực.

• Sử dụng firewall hoặc ACL trên router để ngăn chặn truy cập trái phép.

• Mã hóa thông tin sử dụng các giao thức và thuật toán mạnh như SSL/TLS

**10.Ý nghĩa của phân lớp tài sản. Nêu sự liên quan của phân lớp tài sản với chính sách quản lý tài liệu, điều khiển truy xuất.**

- Ý nghĩa:

+ Đảm bảo cho các tài sản được phân lớp đúng theo giá trị

+ Cơ sở cho các chính sách đảm bảo trên các phân lớp

+ Đảm bảo trách nhiệm, và thực thi trách nhiệm quản lý tài sản của người quản lý

+ Đưa ra phân lớp riêng theo đặc thù

- Ví dụ minh họa phân lớp tài sản thông tin:

+ Bí mật:

• Hồ sơ bảo hiểm y tế (kể cả hồ sơ y tế, kê đơn và tâm lý)

• Kế hoạch hoạt động cụ thể, kế hoạch tiếp thị

• Doanh thu, chi phí, lợi nhuận hoặc các kết quả tài chính khác không được công khai

• Hồ sơ cán bộ, thông tin khách hàng

• Chiến lược kinh doanh

• Những thay đổi lớn trong cơ cấu quản lý công ty

• Những thông tin đòi hỏi kỹ năng hoặc đào tạo đặc biệt

+ Nội bộ:

• Thông tin hoạt động kinh doanh/báo cáo

• Danh sách điện thoại công ty

• Chính sách, tiêu chuẩn, thủ tục

• Thông báo nội bộ

+ Công khai:

• Báo cáo thường niên

• Bản tinh dịch vụ công cộng, tài liệu quảng cáo tiếp thị

**11.Ý nghĩa điều khiển truy xuất, các vấn đề trong quản lý truy xuất người dùng.**

- Ý nghĩa:

+ Đảm bảo việc truy xuất đến tài nguyên của hệ thống

+ Đảm bảo quá trình triển khai cho hệ thống của các chính sách ở trên

+ Sử dụng các cơ chế về mặt kỹ thuật, con người để đảm bảo các cơ chế đã được mô tả

+ Đưa ra nhân tố chính trong thực thi các chính sách đã mô tả

- Các vấn đề trong quản lý truy xuất người dùng:

a. Cơ chế quản lý

- Quản lý truy xuất theo chính sách

+ Mô hình dán nhãn

+ Bảo vệ theo nhóm đã phân

- Quản lý tùy biến

+ Theo mô hình dữ liệu mô tả

+ Hạn chế mô hình cấp quyền tùy biến

b. Quy trình quản lý

- Cấp phép tài khoản

+ Kiểm tra đăng ký tài khoản

+ Cung cấp truy vấn đầu tiên với hệ thống

- Quản lý ưu tiên truy xuất

+ Đảm bảo kiểm tra các ưu tiên theo thời gian với người dùng

+ Đảm bảo sự tồn tại người dùng với thực tế

+ Cơ chế loại bỏ quyền nhanh chóng với các cá nhân

- Quản lý xác thực tài khoản

+ Thay mật khẩu theo tiêu chuẩn công nghiệp: 30 ngày

+ Thời gian thay mật khẩu -> sự cần thiết bảo mật đối với thông tin

+ Mật khẩu được lựa chọn tốt: >= 8 ký tự, không dùng từ trong từ điển

+ Hỗ trợ đăng nhập 1 lần

c. Cơ chế xác thực

- Người dùng có: Thẻ thông minh, thẻ từ, chứng minh thư…

- Xác thực người dùng: Vân tay, võng mạc, hình học tay,…

- Người dùng biết: mật khẩu, PIN, …

d. Thông báo chính xác giới hạn quyền, nghĩa vụ tham gia hệ thống

- Kiểm soát thao tác

- Kiểm soát thông tin người dùng

**12. Ý nghĩa bảo mật vật lý, ví dụ chính sách bảo mật vật lý**

- Ý nghĩa:

+ Bảo vệ hệ thống trước đe dọa vật lý

+ Phòng ngừa để bảo vệ việc truy xuất thiết bị toàn bộ tổ chức

+ Đảm bảo không có sự hư hỏng và thay đổi các thiết bị mà thông tin được lưu trữ

+ Việc xây dựng bảo vệ vật lý cho trung tâm dữ liệu phải tương ứng với giá trị dư

liệu được lưu trữ trong đó.

- Ví dụ chính sách bảo mật vật lý

+ Các máy chủ, các thiết bị truyền thông: Router, moderm, firewall phải được đặt trong phòng máy riêng được bảo vệ tốt kể cả yêu cầu về nhiệt độ, độ ẩm theo đúng khuyến cáo của sản phẩm

+ Đảm bảo nguồn điện luôn được cung cấp

+ Hệ thống UPS cung cấp nguồn khi mất điện lưới trong thời gian ngắn và làm nhiệm vụ chuyển tiếp sang hệ thống máy phát điện dự phòng

+ Giám sát môi trường theo các chỉ số nhiệt độ, độ ẩm, bụi và những mối đe dọa môi trường vật lý khác

+ Lựa chọn cấp nguồn qua Ethernet giảm việc phải đi cáp tới các thiết bị chuyên dụng

+ Các dạng cảnh báo khác nhau cho phép gửi thông báo qua quản trị SNMP, các hệ thống mail, máy chủ web, điện thoại,…

+ Kiểm soát vào ra phòng máy chủ, kiểm soát truy cập hệ thống bằng công nghệ thông minh như camera giám sát, camera hồng ngoại, cảm biến,.v…

+ Chỉ có những người thuộc nhóm quản trị hệ thống hoặc người trực ca mới được phép vào và thao tác trên các máy chủ trong phòng máy. Các cá nhân khác chỉ được vào phòng máy khi được cho phép bởi người quản trị hệ thống hoặc người trực phòng máy.

**13. Ý nghĩa của phân tích nguy cơ, tiến trình phân tích quản lý nguy cơ**

- Khái niệm Nguy cơ: là khả năng bất lợi có thể xảy ra cho hệ thống

- Ý nghĩa:

+ Phân tích được các nguy cơ, mức độ ưu tiên của các nguy cơ, từ đó đánh giá, đưa ra các xử lý tương ứng.

+ Chọn chiến lược phù hợp với giá trị tài sản, chi phí chiến lược < lợi ích thu được từ tài sản

+ Không có mục đích loại bỏ tất cả các nguy cơ mà nhằm mục đích giảm nguy cơ đến mức tối thiểu có thể được.

- Tiến trình phân tích, quản lý nguy cơ

+ Xác định nguy cơ

• Xác định tài sản

• Phân loại tài sản

• Xác định những đe dọa

+ Đánh giá nguy cơ

• Xác định lỗ hổng giữ tài sản và mối đe dọa

• Xác định và định giá trị tài sản bị đe dọa

+ Quản lý nguy cơ

• Lựa chọn chiến lược

• Chứng minh điều khiển

• Giám sát và quản lý thực hiện

Quá trình này được thực hiện lặp lại theo thời gian (tài sản, đe dọa, ưu tiên, giải pháp đã bị thay đổi)

**14. Ý nghĩa kế hoạch công việc liên tục, sự liên quan của quá trình phân tích tác động công việc và các bước.**

- Ý nghĩa:

+ Đảm bảo công việc hoạt động trong các tình huống

+ Bao gồm cả kế hoạch phục hồi sự cố

+ Có tác dụng trong tình huống khẩn cấp

• Khó kiểm tra

• Khó thuyết phục người quản lý

• Bảo hiểm chỉ giải quyết về mặt kinh tế

- Sự liên quan của quá trình phân tích tác động công việc: có nhiều yếu tố ảnh hưởng đến hoạt động

• Thảm họa tự nhiên: Lũ lụt, động đất, hỏa hoạn,v…

• Tai nạn

• Cạnh tranh, tấn công đối thủ

• Năng lượng không được cung cấp

• Các dịch vụ: kết nối, vận chuyển, bảo vệ không hoạt động

• Thảm họa về môi trường

• Tấn công của hacker

- Các bước tiến hành:

+ Xác định các tài nguyên

+ Xác định các đe dọa

+ Xác định các nguy cơ

+ Xác định ảnh hưởng đến hệ thống

+ Xác định các dịch vụ và hệ thống cần được khôi phục ngay

+ Xác định tài nguyên để hồi phục hệ thống

**15. Nêu lý do vì sao phải thiết lập chính sách, tiêu chuẩn, chỉ dẫn về an toàn và đảm bảo thông tin trong doanh nghiệp.**

- Các vấn đề của an toàn và bảo mật xảy ra trong suốt quá trình hình thành, phát triển, tồn tại của hệ thống. Trong chuỗi mắt xích bảo vệ, sức mạnh chuỗi bảo vệ chính là điểm yếu nhất của nó.

- Bảo vệ dữ liệu: hiện nay các biện pháp tấn công ngày càng tinh vi, sự đe dọa tới độ an toàn thông tin có thể đến từ nhiều nơi theo nhiều cách, vì thế chúng ta nên đưa ra các chính sách và chỉ dẫn đề phòng cần thiết.

- Bảo vệ các tài nguyên sử dụng trên mạng: Sau khi làm chủ được hệ thống bên trong, kẻ tấn công có thể sự dụng các máy này để phục vụ cho mục đích của mình như dò mật khẩu người sử dụng, sử dụng liên kết mạng sẵn có để tiếp tục tấn công hệ thống khác.

- Bảo vệ danh tiếng doanh nghiệp, cơ quan: Trong trường hợp người quản trị hệ thống chỉ được biết đến sau khi chính hệ thống của mình được dùng làm bàn đạp để tấn công các hệ thống khác, thì sẽ để lại tổn thất về uy tín và hậu quả lâu dài.

- Chính sách, tiêu chuẩn, chỉ dẫn về an toàn và đảm bảo thông tin sẽ hướng dẫn giải quyết các vấn đề liên quan đến con người:

+ Cơ sở để xem xét các hành động của con người để đánh giá

+ Kết hợp với các giải pháp kỹ thuật quản lý toàn bộ hệ thống

+ Nền tảng cho việc triển khai chương trình an toàn vào bảo mật hệ thống thông tin.

 Nhìn chung cuối cùng là tránh tổn thất cho các doanh nghiệp về mặt dữ liệu, tài

nguyên, danh tiếng, uy tín,.v..v..

**16. Sự tương ứng của phân tích nguy cơ và quá trình phát triển hệ thống? Vòng đời của bảo mật thông tin.**

- Sự tương ứng của phân tích nguy cơ và quá trình phát triển hệ thống:

+ Phân tích nguy cơ chính thức cung cấp các tài liệu thẩm định hệ thống, cho phép doanh nghiệp kiểm soát vận mệnh của riêng mình.

+ Không ai biết hệ thống rõ hơn những người phát triển và chạy chúng, vậy nên, để phân tích nguy cơ, cũng là công việc của chính những người phát triển hệ thống.

+ Phân tích nguy cơ có thể được sử dụng để xem xét lại bất cứ nhiệm vụ, dự án hoặc ý tưởng trong quá trình phát triển hệ thống.

+ Lợi ích lớn nhất của phân tích nguy cơ là xác định có hay không vấn đề để tiến hành tùy trình kế hoạch phát triển hệ thống

+ Quá trình phát triển hệ thống có xảy ra lỗ hổng hay lỗi gì hay không là do có được phân tích đầy đủ các nguy cơ hay không.

- Vòng đời của bảo mật thông tin

- Cost/Benefit Implementation: chi phí, lợi ích thực hiện

- Vulnerability Assessment: đánh giá tổn thương, nguy hại

- Risk Analysis: phân tích nguy cơ

+ Thông thường, kết quả phân tích nguy cơ sẽ được sử dụng trên 2 lần:

• Khi một quyết định cần phải được thực hiện

• Khi có phát sinh và cần phải kiểm tra quá trình ra quyết định

**17. .Tiêu chuẩn ISO 27000 là gì, ý nghĩa của việc áp dụng tiêu chuẩn này. Sự liên quan giữa tiêu chuẩn và chất lượng sản phẩm của hệ thống.**

Dòng tiêu chuẩn ISO 27000

Định nghĩa: là tiêu chuẩn quốc tế về thông tin hoặc quản lý an ninh

 Tiêu chuẩn vạch ra phương pháp để thực hiện đánh giá độc lập hệ thống quản lý an ninh thông tin và chứng nhận cho hệ thống đó

Mục đích: là đưa ra các khuyến nghị về quản lý bảo mật thông tin

 Cung cấp một cơ sở chung để phát triển an ninh của tổ chức

**Phần 2: Câu hỏi về phần kỹ thuật liên quan đến an toàn và bảo mật hệ thống thông tin**

**1.Điều khiển truy cập bắt buộc, tùy quyền, xác thực, ủy quyền là gì**

Điều khiển truy cập bắt buộc (MAC): được dùng để bảo vệ dữ liệu cần được bảo mật cao trong một môi trường mà các dữ liệu và người dùng đều được phân loại rõ ràng

Ví dụ: để đọc file hệ thống, cần phải truy cập quyền root.

Điều khiển truy cập tùy quyền (DAC): được thực hiện theo quyết định hoặc tùy chọn của người dùng dữ liệu

Ví dụ: sinh viên đăng nhập quyền user, phòng đào tạo đăng nhập quyền admin vào hệ thống quản lý điểm

SV - RBAC, RDAC

Các bước trong điều khiển truy cập:

i. Định danh (Identification): Người dùng cung cấp danh định tới hệ thống để xác thực. Ví dụ: người dùng cung cấp username, số điện thoại, email, ...

ii. Xác thực (Authentication): Người dùng chứng minh danh định đó là đúng. Ví dụ: người dùng cung cấp mật khẩu, dấu vân tay, giọng nói,Số PIN ...

iii. Ủy quyền (Authorization): Xác định quyền mà người dùng có. Ví dụ: người dùng được sử dùng quền xem hoặc sửa hoặc xóa một tài nguyên nào đó của hệ thống.

**2.Firewall là gì, phần loại firewall**

Là một công nghệ cho phép ngăn chặn các thông tin cụ thể di chuyển giữa bên trong và bên ngoài hệ thống

Bức tường lửa có thể là:

 Hệ thống máy tính hoặc một thiết bị riêng

 Dịch vụ phần mềm đang chạy trên bộ định tuyến hoặc máy chủ

 Mạng riêng chứa các thiết bị hỗ trợ

Phân loại bức tường lửa:

i. Packet filtering (Tường lửa lọc gói tin): là tường lửa kiểm tra thông tin tiêu đề (header) của gói tin

- Việc kiểm tra dựa trên sự kết hợp của IP nguồn, IP đích hoặc hướng di chuyển của gói tin (hướng vào, ra), hoặc dựa trên giao thức truyền tin TCP, UDP kết hợp kiểm tra các cổng được sử dụng

- Chế độ này sử dụng các quy tắc được thiết kế để cấm các gói với một số địa chỉ hoặc một phần địa chỉ nhất định

a) Lọc tĩnh: các luật được thiết kế trước, nó sẽ quyết địch gói tin nào được phép hoặc từ chối di chuyển qua nó

b) Lọc động: cho phép tường lửa phản ứng lại các sự kiện, hoặc tự tạo ra các luật để điều khiển các sự kiện đó

c) Kết hợp trạng thái: tường lửa theo dõi từng kết nối mạng giữa các hệ thống bên trong và bên ngoài bằng bảng trạng thái. Nó không những kiểm tra các đặc điểm của gói tin mà lưu giữ và kiểm tra trạng thái của các gói tin đi qua

ii. Application gateways (Tường lửa cổng ứng dụng)

Định nghĩa: còn được gọi là các máy chủ proxy, chúng có thể lọc gói ở lớp ứng dụng trong mô

hình OSI. Các gói vào hoặc ra không thể truy cập các dịch vụ mà không có proxy.

iii. Circuit gateway firewall

- Thực thi ở tầng giao vận

- Nó không xem được luồng giữ liệu giữa 2 mạng

- Ngăn chặn kết nối trực tiếp giữa 2 mạng

iv. MAC layer firewalls

- Thực thi ở tầng liên kết

- Cho phép lọc theo một danh sách các chủ biết trước theo địa chỉ MAC

iv. Hybrid firewalls

- Là tường lửa kết hợp 4 loại ở trên như lọc gói, lọc MAC, lọc cổng, hoặc circuit gateways

- Hoặc kết hợp các loại tường lửa trên song song

3. Hệ thống IDS, IPS là gì

IDS là hệ thống phát hiện các dấu hiệu của tấn công xâm nhập, đồng thời có thể khởi tạo các hành động trên thiết bị khác để ngăn chặn tấn công. Khác với tường lửa, IDS không thực hiện các thao tác ngăn chặn truy xuất mà chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo cho người quản trị mạng. Một điểm khác biệt khác đó là mặc dù cả hai đều liên quan đến bảo mật mạng, nhưng tường lửa theo dõi sự xâm nhập từ bên ngoài và ngăn chặn chúng xảy ra, nó giới hạn truy nhập giữa các mạng để ngăn chặn sự xâm nhập nhưng không phát hiện được cuộc tấn công từ bên trong mạng. Bên cạnh đó IDS sẽ đánh giá sự xâm nhập đáng ngờ khi nó đã diễn ra đồng thời phát ra cảnh báo, nó theo dõi được các cuộc tấn công có nguồn gốc từ bên trong một hệ thống.

Chức năng ban đầu của IDS chỉ là phát hiện các dấu hiện xâm nhập, do đó IDS chỉ có thể tạo ra các cảnh báo tấn công khi tấn công đang diễn ra hoặc thậm chí sau khi tấn công đã hoàn tất. Càng về sau, nhiều kỹ thuật mới được tích hợp vào IDS, giúp nó có khả năng dự đoán được tấn công (prediction) và thậm chí phản ứng lại các tấn công đang diễn ra (Active response).

Hai thành phần quan trọng nhất cấu tạo nên hệ thống IDS là sensor (bộ cảm nhận) có chức năng chặn bắt và phân tích lưu lượng trên mạng và các nguồn thông tin khác để phát hiện dấu hiệu xâm nhập (signature); signature database là cơ sở dữ liệu chứa dấu hiệu của các tấn công đã được phát hiện và phân tích. Cơ chế làm việc của signature database giống như virus database trong các chuơng trình antivirus, do vậy, việc duy trì một hệ thống IDS hiệu quả phải bao gồm việc cập nhận thường xuyên cơ sở dữ liệu này.

Một Hệ thống Ngăn ngừa xâm nhập (IPS) là gì ?

Các Hệ thống Ngăn ngừa Xâm nhập

Hai kiểu IPS được biết trên thị trường hiện nay là “dựa vào máy chủ” và “nội tuyến” (dựa vào mạng). Các hệ thống “dựa vào máy chủ” là các phần mềm ngăn ngừa xâm nhập được viết để “móc” trực tiếp vào trong các ứng dụng hay cài đặt trực tiếp trên các máy chủ ứng dụng. Bài viết này chỉ tập trung vào bảo mật “nội tuyến”. Bảo mật “nội tuyến” tương tự như trong kiến trúc tường lửa di trú kép hay một cổng chống vi rút được đặt ngược chiều từ các ứng dụng được bảo vệ và áp dụng các dịch vụ ngăn ngừa xâm nhập cho nhiều ứng dụng xuôi chiều của các IPS. Theo đúng nghĩa của khái niệm này, ta có thể định nghĩa như sau“Một Hệ thống Ngăn ngừa Xâm nhập “nội tuyến” (inline) là bất kỳ một thiết bị phần cứng hay phần mềm nào có khả năng phát hiện và ngăn ngừa các cuộc tấn công đã quen biết”. Thậm chí đơn giản hơn, “Ngăn ngừa Xâm nhập” chỉ đề cập đến việc phát hiện và sau đó ngăn chặn những cuộc tấn công chuyên biệt ứng dụng đã biết. Thuật ngữ “Hệ thống Ngăn ngừa Xâm nhập” (Intrusion Prevention System) bản thân được sử dụng để hợp nhất cả hai khái niệm “Hệ thống Phát hiện” (detection system) và “Hệ thống Ngăn ngừa” (prevention system) dưới một cấu trúc. Chú ý rằng định nghĩa này chỉ nhằm vào các cuộc tấn công đã quen biết.

Phát hiện và ngăn ngừa

Nhìn bề ngoài, các giải pháp phát hiện xâm nhập và ngăn ngừa xâm nhập xuất hiện theo kiểu cạnh tranh nhau. Rốt cuộc, chúng chia sẻ một danh sách các chức năng giống nhau như kiểm tra gói tin, phân tích có trạng thái, ráp lại các đoạn, ráp lại các TCP-segment, kiểm tra gói tin sâu, xác nhận tính hợp lệ giao thức và thích ứng chữ ký. Một IPS hoạt động giống như một người bảo vệ gác cổng cho một khu dân cư, cho phép và từ chối truy nhập dựa trên cơ sở các uỷ nhiệm và tập quy tắc nội quy nào đó. Một IDS (hệ thống phát hiện xâm nhập) làm việc giống như một xe tuần tra bên trong khu dân cư, giám sát các hoạt động và tìm ra những tình huống bất bình thường. Dù mức độ an ninh tại cổng vào khu dân cư mạnh đến mức nào, xe tuần tra vẫn tiếp tục hoạt động trong một hệ thống giám sát và sự cân bằng của chính nó.

Phát hiện xâm nhập

Mục đích của “phát hiện xâm nhập” là cung cấp sự giám sát, kiểm tra, tính pháp lý và báo cáo về các hoạt động của mạng. Nó hoạt động trên các gói tin được cho phép thông qua một thiết bị kiểm soát truy nhập. Do những hạn chế về độ tin cậy và những đe doạ bên trong, “Ngăn ngừa Xâm nhập” phải cho phép một số “vùng xám” (gray area) tấn công để tránh các trường hợp báo động giả. Mặt khác, những giải pháp IDS được “nhồi” trí thông minh có sử dụng nhiều kỹ thuật khác nhau để nhận biết những cuộc xâm nhập, những khai thác, lạm dụng bất chính và các cuộc tấn công tiềm tàng. Một IDS có thể thực hiện các hoạt động mà không làm ảnh hưởng đến các kiến trúc tính toán và kết nối mạng.

Bản chất bị động của IDS nằm ở chỗ cung cấp sức mạnh để chỉ đạo phân tích thông minh các lưu lượng gói tin. Những vị trí IDS này có thể nhận ra :

- Các cuộc tấn công quen biết theo đường chữ ký (signature) và các quy tắc.

- Những biến thiên trong lưu lượng và phương hướng sử dụng những quy tắc và phân tích thống kê phức tạp.

- Những biến đổi mẫu lưu lượng truyền thông có sử dụng phân tích luồng.

- Phát hiện hoạt động bất bình thường có sử dụng phân tích độ lệch đường cơ sở (baseline deviation analysis).

- Phát hiện hoạt động đáng nghi nhờ phân tích luồng, các kỹ thuật thống kê và phát hiện sự bất bình thường.

Ngăn ngừa xâm nhập

Như được đề cập trước đây, các giải pháp “Ngăn ngừa Xâm nhập” nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe doạ tấn công bằng việc loại bỏ những lưu lượng mạng có hại hay có ác ý trong khi vẫn cho phép các hoạt động hợp pháp tiếp tục. Mục đích ở đây là một hệ thống hoàn hảo – không có những báo động giả nào làm giảm năng suất người dùng cuối và không có những từ chối sai nào tạo ra rủi ro quá mức bên trong môi trường. Có lẽ một vai trò cốt yếu hơn sẽ là cần thiết để tin tưởng, để thực hiện theo cách mong muốn dưới bất kỳ điều kiện nào. Điều này có nghĩa các giải pháp “Ngăn ngừa Xâm nhập” được đặt vào đúng vị trí để phục vụ với:

- Những ứng dụng không mong muốn và những cuộc tấn công “Trojan horse” nhằm vào các mạng và các ứng dụng cá nhân, qua việc sử dụng các nguyên tắc xác định và các danh sách điều khiển truy nhập (access control lists).

- Các gói tin tấn công giống như những gói tin từ LAND và WinNuke qua việc sử dụng các bộ lọc gói tốc độ cao.

- Sự lạm dụng giao thức và những hành động lảng tránh – những thao tác giao thức mạng giống như Fragroute và những khảo sát lấn TCP (TCP overlap exploits) – thông qua sự ráp lại thông minh.

- Các tấn công từ chối dịch vụ (DOS/DDOS) như “lụt” các gói tin SYN và ICMP bởi việc sử dụng các thuật toán lọc dựa trên cơ sở ngưỡng.

- Sự lạm dụng các ứng dụng và những thao tác giao thức – các cuộc tấn công đã biết và chưa biết chống lại HTTP, FTP, DNS, SMTP .v.v. – qua việc sử dụng những quy tắc giao thức ứng dụng và chữ ký.

- Những cuộc tấn công quá tải hay lạm dụng ứng dụng bằng việc sử dụng các hữu hạn tiêu thụ tài nguyên dựa trên cơ sở ngưỡng.

Tất cả các cuộc tấn công và trạng thái dễ bị tấn công cho phép chúng tình cờ xảy ra đều được chứng minh bằng tài liệu. Ngoài ra, những khác thường trong các giao thức truyền thông từ mạng qua lớp ứng dụng không có chỗ cho bất cứ loại lưu lượng hợp pháp nào, làm cho các lỗi trở thành tự chọn lọc trong ngữ cảnh xác định.

**4. Phân loại mạng không dây, cơ chế xác thực, lọc địa chỉ MAC, mã hóa sử dụng trong mạng không dây 5**

Phân loại mạng ko dây

1.Tốc độ:11/54/106Mbps

2.Bảo mật: Không đảm bảo bằng mạng có dây do phát sóng thông tin ra mọi phía

3.Thi công: Nhanh và dễ dàng

4.Khả năng mở rộng: Khả năng mở rộng khoảng cách tốt với chi phí hợp lý

5.Tinh mềm dẻo: Các vị trí kết nối mạng có

thể thay đổi mà không cần phải thiết kế lại

Lọc địa chỉ MAC

- Kiểm soát truy cập bằng cách chỉ cho phép các máy tính có các địa chỉ MAC khai báo trước được kết nối đến mạng.

- Địa chỉ MAC có thể bị giả mạo.

- Phải duy trì và phân phối một danh sách các địa chỉ MAC đến tất cả các Access Point.

- Không phải là giải pháp khả thi cho các ứng dụng công cộng. Mã hóa(TKIP/MIC)

TKIP- Temporal Key Integrity Protocol.

- Sửa lỗi phục hồi khóa trong WEP. Bảo vệ IV bằng cách loại bỏ khả năng dự đoán.

- Sử dụng thuật toán mã hóa RC4 như WEP.

- Thêm MIC ở cuối của mỗi thông điệp bản rõ nhằm đảm bảo thông điệp đó không bị giả mạo.

MIC

- Message Integrity Code.

- Chống lại tấn công bit-flip.

- Phải được hiện thực trên client & AP.

Mã hóa (TKIP/MIC)

- Dùng khóa 64 bits

- Chia gói tin thành các khối 32 bits

- Dùng shifts, XORs, + đến mỗi khối 32 bits để lấy ra thẻ xác thực 64 bits

- Khóa MIC được tính toán trên dữ liệu địa chỉ nguồn và địa chỉ đích

- MIC = MIC\_key(SA, DA, PlainMSDU)

- Tránh bắt gói, thay đổi và gởi lại các gói tin

Mã hóa (TKIP/MIC)

- Mỗi khóa mã hóa trên mỗi gói.

- IV có chiều dài 48bits dẫn đến giảm việc tái sử dụng

IV.

- IV mã hóa trước khi gởi.

- MIC thay thế CRC.

- Có thể nâng cấp dể dàng cho phần cứng hỗ trợ WEP.

Mã hóa (TKIP)

Authentication (PSK - Pre-shared key)

- Chế độ đặc biệt (không có hạ tầng 802.1x)

- Passphrase được cung cấp trên tất cả máy trạm và các Access Point

- Dựa trên bắt tay khóa bốn lần

+ Hai lần đầu: máy trạm và access point trao đổi các giá trị ngẫu nhiên để xác thực lẫn nhau.

+ Hai lân kế tiếp : access point hướng dẫn máy trạm để cài đặt khóa được tính toán trước. Máy trạm xác nhận.

**5. Nêu một số thuật toán mã hoá cổ điển, phân tích khả năng áp dụng mô hình cho mã hoá dữ liệu lưu trữ và mã hoá dữ liệu trên đường truyền.**

- Hệ thống mã hóa (Cryptosytem) là một bộ năm (P, C, K, E, D) thỏa mãn các điều

kiện sau:

+ Tập nguồn P là tập hữu hạn tất cả các bản tin nguồn cần mã hóa có thể có

+ Tập đích C là tập hữu hạn tất cả các bản tin có thể có sau khi mã hóa

+ Tập khóa K là tập hữu hạn các khóa có thể được sử dụng

+ E, D là tập luật mã hóa và giải mã. Với mỗi khóa k tồn tại 1 luật mã hóa ek thuộc E và luật giải mã tương ứng dk thuộc D.

Luật mã hóa ek : P -> C và dk: C -> D thỏa mãn dk(ek(x)) = x với mọi x thuộc P

- Một số kỹ thuật mã hóa cổ điển:

1. Mã hóa dịch vòng: Thông điệp được mã hóa bằng cách dịch chuyển xoay vòng từng ký tự đi k vị trí trong bảng chữ cái.

- Cho P = C = K = Zn với mỗi khóa K định nghĩa :

ek(x) = (x + k)mod n và dk(y) = (y - k)mod n với x,y thuộc Zn

- E = {ek, k thuộc K} và D = {dk, k thuộc K}

- Thực hiện đơn giản

- Không gian khóa bé(26), dễ tấn công: vét cạn, thống kê ký tự

2. Mã hóa thay thế : Phương pháp này thực hiện việc mã hóa thông điệp bằng cách hoán vị các phần tử trong bảng chữ cái hay tổng quát hơn là hoán vị các phần tử trong tập nguồn P.

- Cho P=C = Zn: K là tập hợp tất cả các hoán vị n phần tử 0, 1, …n-1.

Như vậy mỗi khóa thuộc K là 1 hoán vị của n phần tử 0, 1, …n-1. Với mỗi khóa k thuộc K, định nghĩa:

ek(x) = π(x)

dk(y) = π-1(y) với x, y thuộc Zn, E = {ek, k thuộc K} và D = {dk, k thuộc K}

- Thời gian thực hiện ngắn

- Không gian khóa là n! khá lớn

- Tấn công theo phương pháp thống kê

3. Mã hóa Affine

- P=C=Zn

- K={(a,b)thuộc Zn x Zn gcd(a,n)=1}

ek(x) = (ax+b) mod n

dk(x) = (a-1(y-b)) mod n

x,y thuộc Zn

E = {ek, k thuộc K} và D = {dk, k thuộc K}

- Trường hợp riêng của thay thế

- Tính toán đơn giản

- Số lượng khóa không lớn

4. Phương pháp Vigenere

P=C=K=(Zn)m

• K={(k1, k2,… ,kr)  (Zn)r}

• ek(x1, x2, ..xr)=((x1+k1) mod n, …,(xr+kr) mod n)

• dk(y1, …, yr)=((y1-k1) mod n), …,(yr-kr) mod n)

- Thuật toán này là mở rộng thuật toán dịch vòng với khóa là bộ nhiều khóa dịch vòng

- Thực hiện đơn giản

- Không gian khóa lớn nm

5. Phương pháp Hill

P=C=(Zn)m

• K là tập hợp ma trận mxm khả nghịch\ek = x\*k

- Thực hiện đơn giản (dựa phép nhân ma trận)

- Không gian khóa lớn nmxm

6. Phương pháp hoán vị

P=C=(Zn)m

•  K là một hoán vị

• e(x1, …, xm) = (x(1), …, x(m))

• d(y1, …, ym)=(y-1(1), …, y-1(m)) 19

• Trường hợp riêng của mã hóa Hill

• Thực hiện đơn giản

• Không gian mã hóa là m!

**6. Khác nhau giữa mã hoá đối xứng và mã hóa bất đối xứng. Nguyên lý của hàm băm, khả năng sử dụng hàm băm trong bảo vệ dữ liệu và các hệ thống ứng dụng**

- Khác nhau giữa mã hóa cổ điển và các hàm băm

Mã hóa cổ điển Hàm băm

Từng ký tự hay nhóm ký tự được thay thế bằng một hay 1 nhóm ký tự khác. Vẫn giữ nguyên độ dài thông tin gốc. Biến đổi khối thông tin gốc có độ dài bất kỳ thành đoạn thông tin có đội dài cố định gọi là mã băm.

- Nguyên lý hàm băm:

+ Biến đổi khối thông tin gốc có độ dài bất kỳ thành một đoạn thông tin có độ dài cố định gọi là mã băm. Mã băm được dùng để kiểm tra tính chính xác của thông tin nhận được.

+ Một hàm băm H áp dụng cho khối thông tin M tạo ra kết quả m, được ký hiệu là

H(M) = m.

+ Thông thường, mã băm được gởi kèm với thông tin gốc, cùng với một cơ chế bảo vệ nào đó giúp mã băm không bị thay đổi hoặc tính lại. Ở phía nhận, hàm băm lại được áp dụng đối với thông tin gốc để tìm ra mã băm mới, giá trị này được so sánh với mã băm đi kèm với thông tin gốc. Nếu hai mã băm giống nhau, nghĩa là thông tin gởi đi không bị thay đổi

- Khả năng sử dụng của hàm băm trong việc bảo vệ dữ liệu và các hệ thống ứng dụng:

+ Ứng dụng chính của hàm băm là sử dụng với các hệ chữ ký điện tử, trong đó thay vì ký trực tiếp lên các văn bản, thông điệp, người ta sẽ ký lên giá trị băm đại diện cho toàn bộ văn bản đó. Ngoài việc sử dụng với các hệ chữ ký điện tử, hàm băm còn được sử dụng vào các mục đích khác như: xác thực hóa thông điệp, xác thực hóa người dùng.

+ Trong các hệ thống yêu cầu có xác thực người dùng, để lưu mật khẩu người ta

cũng sử dụng các hàm băm hoặc các hệ mã trong vai trò của hàm băm.

**7. Cơ sở của mã hoá công khai RSA, phân tích khả năng sử dụng mã hoá RSA để lưu trữ dữ liệu trên hệ thống máy tính, truyền dữ liệu trên mạng máy tính.**

- Cơ sở của mã hóa công khai RSA:

+ Trong phương pháp RSA tất cả các phép tính đều được thực hiện trên Zn

n = pq với p và q là hai số nguyên tố phân biệt.

Cho P = C =Zn và định nghĩa:

K= { ( (n, p, q, a, b): n = pq, p, q là số nguyên tố, ab ≡1 (mod φ(n) ) }

Với mỗi k = (n, p, q, a, b) ∈ K, định nghĩa: ek(x) = xb mod n và dk(y) = ya mod n với x,y ∈ Zn

Giá trị n và b được công bố, trong khi giá trị p, q, a được giữ bí mật

- Phân tích khả năng sử dụng mã hóa RSA để lưu trữ dữ liệu trên hệ thống máy

tính, truyền dữ liệu trên mạng máy tính: (Phan kid bổ sung)

+ Hệ mã RSA có tính an toàn cao nhưng nhược điểm là tốc độ mã hóa chậm. Bởi

vậy nó chỉ được sử dụng với các văn bản ngắn và thường dùng trong giao thức xác

nhận chủ thể (chữ ký điện tử)

+ RSA được áp dụng vào quá trình truyền tải dữ liệu như sau:

• Một khóa riêng sẽ được tạo ra dựa trên các số nguyên tố

• Một khóa chung sẽ được tạo ra dựa trên khóa riêng này theo hàm một

chiều. Tức là việc tìm lại “khóa riêng” từ khóa chung này là một điều gần như không thể. Do đó, khóa chung có thể gửi đi trên mạng

• Khóa chung sẽ được gửi đi trên mạng trong quá trình truyền dữ liệu

• Dữ liệu nhận được sẽ được mã hóa dựa theo khóa chung này, và được giải mã bằng mã riêng.

8. Phân tích sự khác biệt mã hóa cổ điển và mã công khai, khả năng kết hợp giữa hai loại khóa trong truyền tin?

Trong mã hóa cổ điển, thông điệp nguồn được mã hóa với mã khóa k được thống nhất trước giữa người gửi A và người nhận B. Người A sẽ sử dụng mã khóa k để mã hóa thông điệp x thành thông điệp y và gửi y cho người B, người B sẽ sửdụng mã khóa k để giải mã thông điệp y này.

Khóa công khai sử dụng hai loại khóa trong cùng một cặp khóa: khóa công cộng (public key) được công bố rộng rãi và được sử dụng trong mã hóa thông tin, khóa riêng (private key) chỉ do một người nắm giữ và được sử dụng để giải mã thông tin đã được mã hóa bằng khóa công cộng.

Các phương pháp mã hóa cổ điển có ưu điểm xử lý rất nhanh so với các phương pháp mã hóa khóa công khai. Do khóa dùng để mã hóa cũng được dùng để giải mã nên cần phải giữ bí mật nội dung của khóa. Vấn đề khó khăn đặt ra đối với các phương pháp mã hóa này chính là bài toán trao đổi mã khóa.

Ngược lại, các phương pháp mã hóa khóa công khai giúp cho việc trao đổi mã khóa trở nên dễ dàng hơn. Nội dung của public key không cần phải giữ bí mật như đối với khóa bí mật trong các phương pháp mã hóa cổ điển.

Bởi vậy chúng ta có thể sử dụng khóa công khai để mã hóa khóa bí mật, khi đó khóa bí mật có thể được trao đổi an toàn.

9. Trình bày mô hình chữ ký số. Sự cần thiết của triển khai mô hình chữ ký số trong giao dịch điện tử ở Việt Nam. Trình bày hiểu biết về hiện trạng mô hình chữ ký số ở Việt Nam.

- Khái niệm chữ ký số: Chữ ký số là một công nghệ đảm bảo an toàn thông tin dựa trên mật mã khóa công khai cho phép thay thế chữ ký tay và con dấu trên môi trường điện tử.

- Sơ đồ chữ ký số: là bộ 5 (P, A, K, S, V) thỏa mãn các điều kiện dưới đây:

+ P là tập hợp hữu hạn các thông điệp

+ A là tập hợp hữu hạn các chữ ký có thể sử dụng

+ Không gian khóa K là tập hợp hữu hạn các khóa có thể sử dụng

+ Với mỗi khóa k  K, tồn tại thuật toán chữ ký sigk  S và thuật toán xác nhận

chữ ký tương ứng verk  V. Mỗi thuật toán sigk : P -> A và verk: P x A -> {True,

False} là các hàm thỏa điều kiện:

Mọi x thuộc P, y thuộc A: ver(x,y) = true nếu y = sig(x), false nếu y khác sig(x)

\*MÔ HÌNH

- Sự cần thiết của triển khai mô hình chữ ký số trong giao dịch điện tử ở Việt Nam:

+ Mỗi ngày, một số lượng lớn giao dịch điện tử được thực hiện thông qua Internet phục vụ cho các hoạt động phát triển kinh tế - xã hội và quan hệ quốc tế,… Đây là một môi trường giao dịch thuận lợi nhưng cũng có nhiều nguy cơ tiềm ẩn về an toàn thông tin. Do không gặp trực tiếp, đối tác giao dịch khó được xác thực chính xác nên có thể bị mạo danh. Ở dạng điện tử, nội dung các văn bản có thể bị thay đổi bởi người không có thẩm quyền. Do đó, các văn bản điện tử không thể dùng làm bằng chứng để đảm bảo các đối tác không chối bỏ các cam kết của mình.

Giao dịch điện tử chỉ có thể thực hiện một cách an toàn và trở thành một phương

tiện trao đổi thông tin hiệu quả trong thời đại thông tin số nếu các biện pháp an

toàn thông tin cho giao dịch điện tử có thể đảm bảo các tính năng: Bảo mật, Nhất

quán, Xác thực và Chống chối bỏ.

+ Các biện pháp an toàn thông tin cho giao dịch điện tử được sử dụng trước đây như sử dụng tên định danh/mật khẩu (ID/Password), mật khẩu sử dụng một lần

(OTP),… đều có hạn chế riêng về tính năng, mức độ đảm bảo và mô hình giao

dịch. Một trong các biện pháp trên là sử dụng mật mã đối xứng để mã hóa tài liệu

điện tử khi trao đổi giữa hai hay nhiều đối tác. Mật mã này sử dụng một khóa

(thường gọi là mật khẩu) để mã và sử dụng chính khóa đó để mở m ã một tài liệu

điện tử (tệp máy tính hay thông điệp dữ liệu). Nhiều phần mềm phổ biến hiện nay

như MS Word, MS Excel, WinRAR, WinZip,… cho phép người dùng sử dụng

biện pháp này để mã hóa nhằm hạn chế người không có thẩm quyền đọc nội dung

tài liệu. Tuy nhiên, do mã và mở mã phải dùng cùng một khóa nên các đối tác trao

đổi thông tin có sử dụng biện pháp an toàn thông tin này cần biết nhau để thống

nhất mật khẩu. Vì thế mật mã đối xứng không hoàn toàn phù hợp với mô hình

giao dịch mở như thương mại điện tử, k hi các đối tác chưa quen nhau có thể có

nhu cầu giao dịch. Ngoài ra, do mật khẩu được chia sẻ giữa các đối tác nên biện

pháp an toàn thông tin này không có tính năng xác thực và chống chối bỏ.

+ Với việc giao dịch điện tử được dùng ngày càng rộng rãi để tr iển khai các loại

hình giao dịch quan trọng như thương mại điện tử, chính phủ điện tử,… chữ ký số

đã được công nhận là biện pháp an toàn thông tin phù hợp nhất cho giao dịch điện

tử xét từ khía cạnh tính năng và mức độ đảm bảo an toàn thông tin cũng như tí nh

khả dụng.

- Hiểu biết về hiện trạng chữ mô hình chữ ký số ở Việt Nam:

Chữ ký số đem lại nhiều lợi ích cho người dân và cộng đồng doanh nghiệp trong các hoạt động phát triển kinh tế - xã hội. Với chữ ký số, nhiều giao dịch kinh tế, thương mại, hành chính được thực hiện theo cách truyền thống được chuyển sang môi trường điện tử, với độ đảm bảo an toàn cao, giảm bớt thời gian và chi phí thực hiện, thuận lợi và dễ dàng quản lý. Tại Việt Nam, sau một thời gian triển khai, đến nay người dân và cộng đồng doanh nghiệp có thể xác định chữ ký số là dạng thể hiện chữ ký tay và con dấu, được công nghệ đảm bảo và được pháp luật bảo hộ. Sau khi Nghị định số 26/2007/NĐ-CP cùng một số văn bản dưới Nghị định ra đời, đến nay khung pháp lý về chữ ký số dần được hình thành và hoàn thiện. Với việc các CA công cộng được Bộ Thông tin và Truyền thông cấp giấy phép và đi vào hoạt động để cung cấp dịch vụ chứng thực chữ ký số, điều kiện để người dân và cộng đồng doanh nghiệp sử dụng chữ ký số tại Việt Nam đã chín được cụ thể hóa hơn.

+ Một ứng dụng điển hình về sử dụng chữ ký số tại nước ta trong thời gian vừa qua là hệ thống kê khai thuế qua mạng do Bộ Tài chính triển khai và đưa và ứng dụng rộng rãi. Phương thức này cho phép doanh nghiệp chỉnh sửa sai sót một cách nhanh chóng, hồ sơ khai thuế có thể được gửi đi từ bất cứ nơi nào có kết nối

mạng, vào bất cứ thời điểm nào trước hạn quy định, với chi phí in ấn, đi lại được

giảm thiểu, thông tin thuế được nhập và tổng hợp nhanh chóng. Việc ứng dụng

chữ ký số cho phép cải cách và hiện đại hóa ngành thuế, giảm tình trạng quá tải,

áp lực cho doanh nghiệp và cơ quan thuế trong thủ tục nộp thuế, tiết kiệm nhân

lực và nguồn lực xử lý, lưu trữ thông tin về thuế. + Tuy nhiên, đối với người dân và cộng đồng doanh nghiệp, trên góc độ chi phí/hiệu quả, lợi ích của việc sử dụng chữ ký số liên quan đến tỷ lệ chi phí sở hữu chứng thư số trên số các ứng dụng chữ ký số. Hiện nay, trung bình giá thuê bao doanh nghiệp phải trả cho để sở hữu một chứng thư số là 1 triệu VNĐ một năm (chứng thư số cho cá nhân có giá thấp hơn). Tuy nhiên, chữ ký số chỉ được sử dụng chủ yếu với mục đích kê khai thuế qua mạng nên đã có ý kiến cho là giá một chứng thư số còn cao trong điều kiện hiện nay. Tuy nhiên, khi số lượng các ứng dụng thiết thực có sử dụng chữ ký số tăng lên, khi đó chi phí sử dụng chữ ký số sẽ giảm và mức giá hiện nay có thể được người dân và doanh nghiệp chấp nhận.

**10.Tấn công mạng, các bước tấn công mạng là gì, trinh sát, quét cổng, dò tìm lỗ hổng….**

1.Tấn công mạng là gì?

Tấn công mạng hay còn gọi là chiến tranh trên không gian mạng. Có thể hiểu tấn công mạng là hình thức tấn công xâm nhập vào một hệ thống mạng máy tính, cơ sở dữ liệu, hạ tầng mạng, website, thiết bị của một cá nhân hoặc một tổ chức nào đó.

Giai đoạn 1 – Trinh sát

Thăm dò thông tin trên hệ thống mục tiêu.

Thu thập các thông tin của hệ thống:

• hệ điều hành

• dịch vụ

• Cổng

• ...

Thu thập passive: Thu thập các thông tin như vị trí địa lý, điện thoại, email của các cá nhân, người điều hành trong tổ chức.

Thu thập active: Thu thập các thông tin về địa chỉ IP, domain, DNS,... của hệ thống

Giai đoạn 1 – Quét hệ thống

Quét thăm dò hệ thống là phương pháp để tìm hiểu hệ thống và thu thập các thông tin như địa chỉ IP cụ thể, hệ điều hành hay các kiến trúc hệ thống mạng.

Giai đoạn 2 – Đột nhập & khai thác

Chiếm quyền điều khiển (Gainning access)

o Mức hệ điều hành/ mức ứng dụng

o Mức mạng

o Từ chối dịch vụ

Giai đoạn 2 – Duy trì điều khiển

Duy trì điều khiển hệ thống (Maitaining access)

Upload/download biến đổi thông tin

Giai đoạn 3 – Tạo cổng hậu

Giai đoạn 3 – Xoá dấu vết

 Xoá dấu vết (Covering tracks)

Sau khi bị tấn công thì hệ thống sẽ lưu lại những vết do attacker để lại. Attacker cần xoá chúng đi nhằm tránh bị phát hiện

**11.Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Port scaning attack, Avesdropping attack, IP spoofing attack**

a)Port Scanning ATACK:

\* Nguyên Lý :

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

- TCP scan: Trên gói TCP/UDP có 16 bit dành cho Port Number điều đó có nghĩa nó có từ 1 – 65535 port. Thường chỉ scan từ

-1 Số phương pháp:

+SYN SCAN:Gửi SYN Vơi 1 thông số port,nhận lại được SYN ACK thì client biết port trên sever đã mở

+FIN SCAN:Client gửi gói FIN với số port nhất định,nhận ACK sever sẽ mở port đó,Sever gửi về gói RST Thì client (máy khách) biết sever đóng port đó

+ NULL Scan Sure: Client sẽ gửi tới Server những gói TCP với số port cần Scan mà không chứa thông số Flag nào, nếu Server gửi lại gói RST thì tôi biết port đó trên Server bị đóng.

+ XMAS Scan Sorry: Client sẽ gửi những gói TCP với số Port nhất định cần Scan chứa nhiều thông số Flag như: FIN, URG, PSH. Nếu Server trả về gói RST tôi biết port đó trên Server bị đóng.

+ TCP CONNECT: gửi đến Server những gói tin yêu cầu kết nối port cụ thể trên server, Nêu server trả về gói SYN/ACK thì mở cổng đó

+ACK SCAN: Scan này nhằm mục đích tìm những Access Controll List trên Server, Client cố gắng kết nối tới Server bằng gói ICMP, nhan được gói tin là Host Unreachable thì client se hiểu port đó trên server đã bị lọc.

\*Chức năng:

- Xác định máy đang mở cổng nào.

-Xác định hệ thống đang sử dụng dịch vụ nào.

\* Một số phương pháp phòng chống:

- Biện pháp đối phó là quá trình hoặc bộ công cụ được sử dụng bởi các quản trị viên an ninh để phát hiện và có thể ngăn chặn port-scanning các máy chủ trên mạng của họ. Danh sách các biện pháp đối phó cần được thực hiện để ngăn chặn một hacker thu thập thông tin từ quá trình quét cổng:

- Kiến trúc an ninh thích hợp, chẳng hạn như thực hiện các IDS và tường lửa nên được đi chung.

-Hacker chân chính sử dụng công cụ của họ thiết lập để kiểm tra việc Scanning, thực hiện các biện pháp đối phó. Khi tường lửa được đặt ra, công cụ aport-scanning nên được chạy cho các máy chủ trên mạng để cho phép tường lửa phát hiện chính xác và dừng các hoạt động của port-scanning.

-Tường lửa có thể phát hiện các hoạt động thăm dò được gửi bởi các công cụ portscanning. Các tường lửa nên tiến hành lấy trạng thái kiểm tra (stateful inspections). Có nghĩa là nó sẽ kiểm tra không chỉ các tiêu đề TCP mà cả dữ liệu của gói tin để xác định liệu được phép đi qua tường lửa.

- Network IDS nên được sử dụng để phát hiện các phương pháp dò tìm hệ điều hành được sử dụng bởi một số công cụ hacker phổ biến như Nmap.

- Chỉ có các cổng cần thiết nên được giữ ở trạng thái mở. Phần còn lại sẽ được lọc hoặc bị chặn.

-Các nhân viên của tổ chức sử dụng các hệ thống cần được đào tạo thích hợp nhận thức về an ninh. Cũng nên biết chính sách bảo mật khác nhau mà họ đang cần làm theo.

b) Eavesdropping Attack: ( tấn công nghe lén)

\*Nguyên Lý :

- Sử dụng các phương pháp vật lý :Nghe trộm qua đường truyền vật lý hoặc sóng vô tuyến

- Nghe lén mạng :

+Tham gia vào mạng

+Nhận các gói tin được truyền tới cổng mạng

+Nếu mạng sử dụng là switch thì dùng phương pháp ‘Man in the midle’

\*Chức năng:

- Tạo ra các gói tin có địa chỉ IP giả

- Vượt qua các kiểm soát nguồn gốc về địa chỉ IP

- Phục vụ các mô hình tấn công khác: kiểu phiên, kiểu phản xạ

\*Một số phương pháp phòng chống:

- Sử dụng switch thay cho hub

- Giám sát địa chỉ MAC

- Sử dụng cơ chế mã hóa truyền tin và mã hóa theo thời gian

- Sử dụng các dịch vụ mã hóa trong liên kết: SSL, SSH, SFTP, HTTPS

- Sử dụng các phần mềm phát hiện hoạt động nghe lén trên mạng

c) IP spoofing attack(Giả mạo địa chỉ IP)

\*Nguyên Lý :

- Tạo ra các gói tin có địa chỉ IP giả mạo không là địa chỉ máy gửi gói tin. Vượt qua các kiểm soát về nguồn gốc địa chỉ ip

- Phục vụ các mô hình tấn công khác: Tấn công về phiên, Tấn công kiểu phản xạ

Attacker có thể gửi các thông điệp đến một máy tính mà dưới danh nghĩa là một host hợp lệ. Ở đây có một vài sự khác nhau trong nhiều cách tấn công theo kiểu này:

+ Giả mạo bằng cách bắt gói(Non Blind spoofing):Phân tích số thứ tự cho máy cùng mạng

+Giả mạo địa chỉ IP từ xa(Blind spoofing):khác mạng có được số TCP sequence chính xác là rất khó,tuy nhiên với 1 số kỹ thuật như định tuyến theo địa chỉ nguồn, máy tấn công cũng có thể xác định chính xác được chỉ số đó.

\*Chức năng:

- Giả mạo IP được thường xuyên nhất được sử dụng trong tấn công từ chối dịch vụ. Trong các cuộc tấn công như vậy, mục tiêu là để làm lụt nạn nhân với lượng truy cập áp đảo, và những kẻ tấn công không quan tâm về việc nhận được câu trả lời cho các gói tin tấn công. Các gói tin với địa chỉ giả mạo là như vậy, thích hợp cho các cuộc tấn công như vậy với mục đích chính là che giấu nguồn gốc thực sự của cuộc tấn công.

- Giả mạo IP còn là một phương pháp tấn công được sử dụng bởi những attacker để đánh bại các biện pháp an ninh mạng, chẳng hạn như xác thực dựa trên địa chỉ IP. Loại tấn công này hiệu quả nhất trong các hệ thống có độ tin cậy giữa các máy cao

\*Một số phương pháp phòng chống:

- Không sử dụng xác thực bằng địa chỉ IP, dùng mật mã xác thực

- Phát hiện các bất thường kết nối mạng

- Dùng danh sách kiểm tra truy cập (ACL) trên các interface của router. Một ACL có thể được dùng để loại bỏ những traffic từ bên ngoài mà lại được đóng gói bởi 1 địa chỉ trong mạng cục bộ

- Mã hóa traffic giữa các thiết bị bằng Ipsec tunnel

**Câu 12: Nguyên lý, khả năng, phương thức phòng chống với các phương**

**thức tấn công mạng máy tính: Hijacking attack, Replay attack, Man-in-the-middle.**

**- Hijacking attack( tấn công chiếm quyền điều khiển)**

+ Nguyên lý: truy cập trái phép thông tin hoặc dịch vụ trong một hệ thống máy tính. Người tấn công bằng 1 cách nào đó xen vào giữa cuộc giao tiếp giữa 2 người. Người tấn công sẽ chiếm quyền của 1 trong 2 người, hoặc chỉ làm gián điệp để lấy thông tin 2 người gửi cho nhau.

+Cách thức:

Nghe lén thông tin liên lạc

Đợi kết thúc quá trình xác thực

Gửi tín hiệu yêu cầu kết thúc

Tiếp tục liên kết với máy còn lại

+ Phương thức phòng chống

Tiến hành mã hóa phiên

Xác thực phiên theo thời gian

- Replay attack( tấn công phát lại)

+ Nguyên lý: Sử dụng công cụ để ghi nhận tất cả thông tin trao đổi khi một máy tính nào đó truy xuất đến server. Sau đó sử dụng các thông tin bắt được trên mạng để nối kết lại đến server đó. Đây là kỹ thuật mà Attacker khi nắm được một số lượng packet sẽ sử dụng lại những packet này sau đó.

Ví dụ Attacker có được packet chứa password của một user. Password này đã được mã hoá và attacker không biết được. Tuy nhiên hệ thống chứng thực không có chức năng kiểm tra Session time hay hệ thống có TCP Sequence number kém. Attacker sẽ thực hiện bỏ qua xác thực (Bypass Authenticate ) bằng cách gửi packet một lần nữa hay còn gọi là replay.

+ Sử dụng thông tin nghe lén

• Lưu trữ

• Gửi lại thông tin đến máy cần để xác thực

+ Phương thức phòng chống

• Xác thực theo phiên (chỉ số phiên)

• Sử dụng phương pháp xác thực lại theo thời gian (sau thời gian kết nối)

- Man – in – the – middle:

+ Nguyên lý: Tấn công khi làm cho hai bên kết nối, hiểu nhầm người thứ 3 là đối tác của mình

+ Các hình thức:

Tấn công bằng bộ phát sống giả mạo (AP)

• Sử dụng bộ phát có sóng mạnh hơn

• Máy kết nối nhầm, hoặc xác thực nhầm

Tấn công bằng làm giả tín hiệu tính hiệu ARP

• Gửi các thông điệp map giữa IP và MAC

Tấn công vào DNS

• Dựa trên cơ chế gửi và nhận địa chỉ IP thông qua tên miền

• Gửi một địa chỉ IP khác với địa chỉ tên miền

+ Phương thức phòng chống cho cả 3 loại này (vì 3 loại này có bản chất giống nhau):

Bảo mật vật lý (Physical security) là phương pháp tốt nhất để chống lại kiểu tấn công này.

Ngoài ra, ta có thể ngăn chặn hình thức tấn công này bằng kỹ thuật mã hoá: mã hoá traffic trong một IPSec tunnel, hacker sẽ chỉ nhìn thấy những thông tin không có giá trị.

**13.Tấn công SQL injection, tràn bộ đệm, chéo trang – cross page attack? Giải pháp phòng chống?**

- Tấn công 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, DB2,...

+ Nguyên nhân: Do việc sử dụng xây dựng câu lệnh SQL trực tiếp

 Chèn vượt qua điều kiện kiểm tra

 Tấn công select

 Chèn thêm các lệnh không mong muốn (multi command)

+ Giải pháp phòng chống:

• Làm sạch dữ liệu đầu vào: Mô hình Blacklist và Whitelist. Cấm những

giá trị input được cho là nguy hiểm và cho phép những giá trị input cho là an

toàn.

• Chuẩn hóa dữ liệu

• Chuỗi: thay thế ký tự ' bằng '' (2 ký tự ')

• Thay thế các ký tự trong trường hợp cộng chuỗi

• Không sử dụng phương pháp cộng chuỗi mà sử dụng

• Stored procedure

• Inline parameter

- Tấn công tràn bộ đệm

+ Tấn công tràn bộ đệm (Buffer overflow attack): là phương thức tấn công vào các lỗi lập trình của phần mềm. Lỗi này có thể do lập trình viên, do bản chất của ngôn ngữ hoặc do trình biên dịch.

+ Nguyên nhân: 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. Gây ra nhiều lỗ hổng bảo mật đối với phần mềm và tạo cơ sở cho nhiều thủ thuật khai thác.

+ Giải pháp phòng chống:

• Thông báo lỗi đủ người dùng hiểu, và xử lý tại thời điểm đó

• Xử lý kiểm lỗi cho các lệnh có nguy cơ: dữ liệu, thiết bị khác, kết nối

• Xử lý các thông tin trả về đầy đủ

• Xây dựng hàm tường minh

• Sử dụng trình biên dịch với các ngôn ngữ bậc cao ít có khả năng bị tấn

công tràn bộ đệm.

• Sử dụng các thư viện an toàn

• Chống tràn bộ nhớ đệm trên stack bằng kỹ thuật Stack-smashing

protection

• Bảo vệ không gian thực thi

• Ngẫu nhiên hóa sơ đồ không gian địa chỉ

- Tấn công Cross page attack (XSS):

+ Là một kỹ thuật tấn công bằng cách chèn vào các website động (ASP, PHP,..) nhưng 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.

+ Giải pháp phòng chống:

• Người dùng cẩn thận khi sử dụng các link được chia sẽ

• Kiểm tra dữ liệu đầu vào loại các thẻ nhạy cảm

• Cấu hình dịch vụ

• Mã hóa các ký tự < , > để vô hiệu hóa Script trước khi insert nó vào

database, tuy bị mã hóa, nhưng lúc hiển thị ra trang web vẫn là dấu < , >.

• Lỗi XSS có thể tránh được khi máy chủ web đảm bảo những trang phát

sinh được mã hóa thích hợp để ngăn chặn chạy những script mong muốn.

**14.Tấn công DoS, DDoS nguyên lý và khả năng phòng chống?**

- NGUYÊN LÝ:

Tấn công DoS(Denial-of-Service\_ Tấn công từ chối dịch vụ):

Một cuộc tấn công dạng Từ-chối-Dịch-vụ /Denial-of-Service (DoS) được thiết kế để ngăn trở hoặc chặn đứng các họat động thông thường của một trang web, máy chủ hoặc tài nguyên mạng khác. Tin tặc có thể dùng nhiều cách khác nhau để thực hiện các cuộc tấn công này. Một phương pháp phổ biến là gửi đến nhiều yêu cầu liên tục vượt quá khả năng xử lý của máy chủ. Việc này sẽ làm cho máy chủ chạy chậm hơn bình thường (website sẽmất nhiều thời gian hơn để mở ra hoặc xử lý thông tin) và có thể phá huỷ hoàn toàn máy chủ (dẫn đến tất cả website trên máy chủ đều bị đánh sập)

Tấn công DDoS(Distributed-Denial-of-Service\_ Tấn công từ chối dịch vụ phân tán):

Một cuộc tấn công dạng Từ-chối-Dịch-vụ-Phân-tán/ Distributed-Denial-of-Service (DdoS) chỉ khác ở chỗ được thực hiện bằng cách sử dụng nhiều máy tính khác nhau. Hacker thường sử dụng một máy tính đã bị xâm nhập, gọi là “máy chủ”, để điều khiển các máy bị xâm nhậm khác, gọi là “zombie” (xác chết biết đi), để thực hiện cuộc tấn công. Cả máy chủ và zombie đều bị hacker xâm nhập bằng cách cài Trojan hay mã độc, thông qua lỗ hổng của một ứng dụng nào đó trên máy.

- CÁCH PHÒNG CHỐNG:

Nguyên tắc chống tấn công DoS là cần phải lọc và gạt bỏ được các luồng tin tấn công và tốt hơn nữa là ngăn chặn được các nguồn tấn công. Để chống DDoS phải vô hiệu hóa được hoạt động của các mạng botnet. Để làm được điều này một cách hiệu quả thường đòi hỏi các biện pháp điều phối ứng cứu sự cố ở quy mô quốc gia hay thậm chí phối hợp nhiều nước. Do đó khi phát hiện có các cuộc tấn công DoS hay DDoS, các đơn vị quản lý cổng/trang TTĐT cần báo cho Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) càng sớm càng tốt. Măt khác, việc áp dụng các biện pháp và công cụ kỹ thuật tại chỗ để nâng cao năng lực bảo vệ các cổng/trang TTĐT cũng có hiệu quả rõ rệt.

Một số biện pháp kỹ thuật và công cụ phòng chống tấn công từ chối dịch vụ:

- Tăng cường khả năng xử lý của hệ thống:

+ Tối ưu hóa các thuật toán xử lý, mã nguồn của máy chủ web

+ Nâng cấp hệ thống máy chủ

+ Nâng cấp đường truyền và các thiết bị liên quan,

+ Cài đặt đầy đủ các bản vá cho hệ điều hành và các phần mềm khác để phòng ngừa khả năng bị lỗi tràn bộ đệm, cướp quyền điều khiển,v.v…

- Hạn chế số lượng kết nối tại thiết bị tường lửa tới mức an toàn hệ thống cho phép.

- Sử dụng các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) để

ngăn chặn các kết nối nhằm tấn công hệ thống.

- Phân tích luồng tin (traffic) để phát hiện các dấu hiệu tấn công và cài đặt các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) ngăn chặn theo các dấu hiệu đã phát hiện.

- Sử dụng hệ thống thiết bị, phần mềm hoặc dịch vụ giám sát an toàn mạng (đặc biệt về lưu lượng) để phát hiện sớm các tấn công từ chối dịch vụ

- Sử dụng thiết bị bảo vệ mạng có dịch vụ chống tấn công DDoS chuyên nghiệp kèm theo, ví dụ như: Arbor, Checkpoint, Imperva, Perimeter,…

**15.Khác nhau giữa virus, worm, trojan, back door, rookit**

\*VIRUS

Là một chương trình, hoặc đoạn chương trình kí sinh trên chương trình khác. Virus nằm trên 1 file.

Thi hành khi file kí sinh được mở, kích hoạt.

Có khả năng tự nhân bản

Nguy hiểm: Tấn công, phá hoại làm hư hại, hỏng, mất dữ liệu,.v…v

Worm

+ Là một file độc lập.

Tự thi hành, tấn công qua danh sách địa chỉ.

Có khả năng tự nhân bản

Nguy hiểm: tương đương với virus, nguy hiểm hơn với tấn công và tự lây lan qua hệ thống mạng.

Trojan

+ Là một chương trình, mã độc nằm chứa trong 1 chương

trình hợp pháp, ẩn trong máy tính

Ẩn trong máy đến khi 1 chương trình khác kích hoạt thì thi hành

Không tự nhân bản

Nguy hiểm: sao chép và khai thác thông tin, dữ liệu của nạn nhân, gửi về cho tin tặc để tin tặc có thể lấy cắp dữ liệu, xóa file,….

Backdoor

+ Là một đoạn chương trình

Khi nhận được lệnh từ ngoài, nó được kích hoạt và phá hoại theo mục đích.

Không tự nhân bản

Nguy hiểm: Mở một dịch vụ nào đó để tạo cổng sau nhằm mục đích dễ dàng đột nhập vào máy tính nạn nhân một cách kín đáo khi cần.

**16.Phương pháp phân tích mã độc tính, động là gì**

Phân tích mã độc là một bước quan trọng trong để có thể ngăn chặn và tiêu diệt hoàn toàn mã độc ra khỏi máy tính và hệ thống mạng; khôi phục lại hiện trạng của mạng như ban đầu; truy tìm nguồn gốc tấn công.

* 1. [Cơ bản] Phân tích tĩnh: Mục tiêu xác định một tệp/ứng dụng có phải mã độc hay không, cung cấp các thông tin cơ bản nhất về các hàm đặc trưng. Có thể hỗ trợ viết các mã nhận diện (Network signatures) mức cơ bản. Đặc trưng của phương pháp này là khả năng phân tích nhanh, không yêu cầu kiến thức chuyên sâu nhưng hạn chế là bỏ qua nhiều đặc tính quan trọng của mã độc.
  2. [Cơ bản] Phân tích động: Mục tiêu là chạy mã độc, theo dõi hành vi mã độc thực hiện trên hệ thống từ đó có phương pháp loại bỏ mã độc và tạo ra các mã nhận diện. Tuy nhiên trước khi phân tích cần thiết lập môi trường phân tích riêng để tránh bị lây nhiễm vào hệ thống thật (Xem chi tiết phương pháp tạo môi trường vào bước tiếp theo). Đặc trưng của phương pháp này cũng tương tự phương pháp phân tích tĩnh ở mức cơ bản: Không yêu cầu nhiều kĩ thuật và kiến thức chuyên môn, nhanh nhưng hiệu quả không cao và có thể bỏ qua nhiều tính năng quan trọng.
* [Nâng cao] Phân tích tĩnh: Thực hiện việc dịch ngược mã độc bằng các công cụ Disassembler, xem nội dung và cấu trúc mã nguồn để xác định xem mã độc làm gì. Đặc trưng của phương pháp này yêu cầu kiến thức về dịch ngược, hệ thống, tập lệnh.
* [Nâng cao] Phân tích động: Sử dụng các trình debugger để nghiên cứu và xem cách thức thực thi của mã độc trong môi trường thật. Từ đó trích xuất thông tin chi tiết về mã độc: nguồn gốc, cách thức lây nhiễm, các đoạn mã, các hàm quan trọng. Để có thể thực hiện được phương pháp này cần trang bị kiến thức chuyên sâu về kĩ thuật, thành thạo việc sử dụng các công cụ và nhiều kĩ năng để có thể vượt qua các kĩ thuật của mã độc.

**17.Khả năng bảo vệ hệ thống của trình quét virus và firewall**

- Khả năng bảo vệ hệ thống của trình quét virus:

+ Virus là một phần mã máy tính tự gắn nó với một chương trình hoặc một tệp để nó có thể phát tán từ máy tính tới máy tính, lây nhiễm khi nó di chuyển. Các vi rút có thể phá hủy phần mềm, phần cứng, và các tệp của bạn.

+ Nguyên lý hoạt động của trình diệt virus:

. Dựa trên database có sẵn: lúc này antivirus sẽ quét ổ cứng kiểm tra

xem coi có file nào có trùng mã hash (thường là md5) với virus có trong database

không? nếu trùng thì nó sẽ delete hoặc cách ly...

. Dùng các thuật toán thông minh: lúc này antivirus sẽ dựa trên cách

thức hoạt động của một chương trình để kiểm tra xem nó có giống với virus hay

không. Ngoài ra, khi quét các file trên một ổ đĩa nào đó, antivirus sẽ không kiểm

tra dựa trên database mà dựa trên các dấu hiệu chung của virus để nhận diện. Dĩ

nhiên nhận diện thông minh sẽ có một sai số nhất định (tỉ lệ nhận lầm file là

virus, hay không nhận diện được virus ...)

- Khả năng bảo vệ hệ thống của firewall: .

+ Tính năng chính của FireWall là

Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong

(Intranet) và mạng Internet. Cụ thể là:

- Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).

- Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào).

**18.IPSec, VPN khả năng bảo vệ thông tin trên đường truyền**

- Khái niệm: IP sercurity dựa trên nền tảng tiêu chuẩn được cung cấp một khóa cho phép bảo mật giữa hai thiết bị mạng ngang hàng.

Hay nói cách khác nó là một tập hợp các chuẩn, các nguyên tắc đã được định nghĩa để kiểm tra, xác thực và mã hóa gói dữ liệu IP để cung cấp cho kênh truyền dẫn mạng bảo mật

+ Sử dụng mã hóa

 Sử dụng mô hình 3DES

 Sử dụng mô hình AES

+ Kiểm tra toàn vẹn

 HMAC-MD5

 HMAC-SHA1

+ VPN: là sự triển khai Ipsec kết nối

 Kết nối site to site

 Remote access (truy cập từ xa)

- Vai trò: Sử dụng thêm các header mới để mô tả được thông tin

+ Mã hóa trong gói tin

+ Thông tin về tính toàn vẹn

+ Sử dụng mô hình truyền khóa để thống nhất khóa

+ Cho phép xác thực hai chiều, trước và trong quá trình truyền tải dữ liệu

+ Mã hóa đường truyền giữa 2 máy tính khi được gửi qua một mạng

+ Bảo vệ gói dữ liệu IP và phòng ngự các cuộc tấn công mạng không bảo mật

+ IPSec bảo vệ các lưu lượng mạng bằng việc sử dụng mã hóa và đánh dấu dữ liệu

- Tính năng, khả năng:

+ Tính xác thực và tính nguyên vẹn dữ liện (Authentication and data integrity) Cung cấp cơ chế mạnh mẽ xác thực của người gửi và kiểm chứng bất ký sự sửa đổi không bảo vệ trước đó của nội dung gói dữ liệu bởi người nhận. Chống lại các tấn công giả mạo, đánh hơi và từ chối dịch vụ

+ Sự cẩn mật (Confidentiality) Mã hóa dữ liệu bằng kỹ thuật mã hóa cao cấp, ngăn người chưa chứng thực truy cập đường truyền

Dùng IPSec tunnel để ẩn IP, nút nguồn, nút đích từ kẻ nghe lén

+ Quản lý khóa: (Key management) IPSec dùng giao thức thứ ba, Internet Key Exchange (IKE), để thỏa thuận các giao thức bảo mật và các thuật toán mã hóa trước và trong suốt phiên giao dịch. IPSec phân phối và kiểm tra các khóa mã và cập nhập những khóa đó khi được yêu cầu.

**19. Các hệ thống sau dùng để làm gì?**

Hệ thống tấn công BPS, Công cụ Burpsuit, Hệ thống Flowmon, Hệ thống Sonicwall TZ400, Hệ thống Addnet, Hệ thống Logrythm

BP là thiết bị được sử dụng để kiểm tra tính năng bảo mật và hiệu năng phòng vệ của các thiết bị/hệ thống bảo mật như firewall ids/ips bằng cách thực hiện tấn công(Ddos,malware,vius…) với lưu lượng cực lớn vào thiết bị được kiểm tra.

Burpsuit là một ứng dụng được dùng để kiểm thử xâm nhập ứng dụng web.

Các tính năng:  
• Interception Proxy: được thiết kế để bắt các  
request gửi lên server.  
• Repeater: cho phép sửa đổi nội dung request  
một cách nhanh chóng.  
• Intruder: tự động hóa việc gửi các payloads lên  
server.  
• Decoder: decode và encode string theo các  
format khác nhau (URL, Base64, HTML,...)

Flowmon là một hệ thống hỗ trợ giám sát và phân tích dữ liệu mạng.

Sonicwall TZ400 là một hệ thống tường lửa firewall next generation với nhiều công nghệ bảo mật tích hợp sâu với nhau thành 1 khối thống nhất

Addnet là hệ thống giúp quản lý mạng,tăng cường an ninh hệ thống.

Logrythm là hệ thống giám sát mạng thông qua việc ptich và quản lý hệ thống log từ các tbi trong 1ht mạng.

2. Bài tập đánh giá rủi ro, tính lợi ích chi phí và đưa ra các chính sách với từng rủi ro cụ thể

Rủi ro = khả năng xảy ra rủi ro \* giá trị tài sản -

phần trăm của các giảm thiểu rủi ro bởi cáckiểm soát hiện tại

+ Sự không hiểu biết chắc chắn về các lỗ hổng hiện tại

Khả năng rủi ro

- Là xác suất của một lỗ hổng cụ thể bị đối phương khai thác hoặc tấn công thành công

- Khả năng sẽ nhận giá trị trong đoạn [0.1, 1]

- Ví dụ: dữ liệu luôn luôn đối mặt với các yếu tố

như:

+ Khả năng hỏa hoạn

+ Khả năng nhận các thư điện tử chứa mã độc

+ Các cuộc tấn công mạng

Định giá trị cho các tài sản thông tin

- Sử dụng các thông tin từ tài sản để đánh trọng

số giá trị cho tài sản

- Giá trị trong khoảng [1, 100]

- 100 có nghĩa là hệ thống ngừng hoạt động

Xác định khả năng kiểm soát các lỗ hổng

- Với mỗi mối đe dọa đưa ra danh sách các ý

tưởng có thể kiểm soát được

- Ước lượng rủi ro còn lại sau khi đã thực hiện các kiểm soát

- Bài toán 1: Tài sản A có điểm giá trị là 50, có 1 lỗ hổng. Lỗ hổng 1 có khả năng xảy ra là 1.0 và hiện tại chưa có kiểm soát nào cho lỗ hổng này, Bạn ước tính giả định với độ chính xác là 90%

- Bài toán 2: Tài sản B có điểm giá trị là 50, có 2 lỗ hổng. Lỗ hổng 2 có khả năng là 0.5 với ước lượng kiểm soát hiện tại là 50%. Lỗ hổng 3 có khả năng là 0.1 và chưa có kiểm soát hiện tại nào. Bạn ước lượng giả định rủi ro với độ chính xác 80%

Rủi ro của A= (50 X 1.0)–(50 X 1.0) X0% + (50 X 1.0) X10%

= (50 X 1.0)– ((50 X 1.0)X0) +((50 X 1.0)+0.1)

= 50 – 0 + 5 = 55

Rủi ro của B (V2)= (100 X 0.5)– (100 X0 .5) X50% + (100 X0 .5) X20%

= 50- 25 + 10 = 35

Rủi ro của B (V3)= (100 X0 .1)– 0% + (100 X0 .1) X20%

= 10 – 0 + 2 = 12

tính lợi ích chi phí và đưa ra các chính sách với từng rủi ro cụ thể

Công thức tính kỳ vọng mất mát đơn:

SLE = asset value \* exposure factor =giá trị tài sản\*yếu tố tiếp xúc

Exposure factor = % loss from exploitation=%mất mát từ khai thác

- Kỳ vọng mất mát hàng năm:

ALE = SLE \* ARO (Tỉ lệ hằng năm xảy ra)

- Hạng mục ảnh hướng tới chi phí điều khiển:

• Chi phí phát triển hoặc mua lại

• Chi phí thực hiện

• Chi phí dịch vụ

• Chi phí bảo trì

Công thức tính lợi ích chi phí (CBA)

CBA xác định có hay không kiểm soát thay thế đang được đánh giá là giá trị phát sinh để kiểm soát lỗ hổng

Công thức:

CBA = ALE (prior) – ALE (post) – ACS

- ALE (trước) là kỳ vọng mất mát hàng năm của rủi ro trước khi thực hiện kiểm soát

- ALE (sau) được ước tính ALE dựa trên sự kiểm soát được đặt ra trong một khoảng thời gian

- ACS là chi phí bảo vệ hàng năm

- CBA >0: nên áp dụng chính sách, ngược lại thì không áp dụng chính sách đó.

Chiến lược kiểm soát rủi ro

Khi sắp xếp xong các rủi ro theo mức độ quan trong, chúng ta phải chọn một trong 4 chiến lược

sau để kiểm soát:

1. Tránh rủi ro bằng cách xóa bỏ, hoặc giảm các

rủi ro. Ví dụ: chặn email ngoài Internet

2. Chuyển rủi ro ra khỏi hệ thống, hoặc bên thứ 3:

Ví dụ mua bảo hiểm

3. Giảm ảnh hưởng của các rủi ro

4. Chấp nhận rủi ro (Hiểu rủi ro nhưng vẫn chấp

nhận)

tránh rủi ro

- Ngăn ngừa việc thực thi các lỗ hổng

- Kiểm soát các mối đe dọa, loại bỏ các tài sản có

chứa lỗ hổng, giới hạn truy cập, thêm các biện

pháp bảo vệ bằng bộ phận bảo vệ

- 3 phương pháp:

+ Áp dụng các chính sách

+ Đào tạo và giáo dục

+ Áp dụng các công nghệ bảo mật mới

Chuyển đổi rủi ro

Bằng cách chuyển các rủi ro cho một bên khác :

- Xem xét lại cách dịch vụ được cung cấp

- Sửa đổi các mô hình triển khai

- Gia công phần mềm

- Mua bảo hiểm

- Thực hiện hợp đồng dịch vụ

Giảm rủi ro

Giảm rủi ro là giảm ảnh hưởng của các lỗ hổng

thông qua các kế hoạch và chuyển bị:

- Kế hoạch phản hồi lại các biến cố

- Kế hoạch phục hồi thảm họa\

- Kế hoạch công việc liên tục

Chấp nhận rủi ro

Không làm gì cả, chập nhận khi rủi ro đến:

- Tình huống xảy ra khi việc đánh đổi chi phí cho

việc áp dụng các biện pháp kiểm soát rủi ro cao

hơn chính tài sản của hệ thống khi thay thế mới

lựa chọn chiến lược kiểm soat rủi ro

- Lựa chọn các mối đe dọa, và giá trị tài sản đóng

vai trò quyết định trong lựa chọn chiến lược:

+ Khi có 1 lỗ hổng, thực hành các kiểm soát để giảm thiểu khả năng của lỗ hổng đó

+Khi một lỗ hổng có thể được khai thác - áp dụng bảo vệ lớp, thiết kế kiến trúc và điều khiển quản trị

+ Khi chi phí của kẻ tấn công ít hơn lợi nhuận tiềm năng - hãy áp dụng biện pháp bảo vệ để tăng chi phí cho kẻ tấn công

+ Khi mất tiềm năng là đáng kể - thiết kế lại kiến trúc mới, điều khiển mới

**Tai sao can dam bao an toan thong tin?**

Vi thong tin la 1 loai tai san (thong tin KH, csdl...) co lien quan den tai san vat ly khac (tien, vang...)

**Bao mat tt**

la su bao ve thong tin cung nhu cac thanh phan cua no nhu he thong, phan cung de su dung, luu tru, truyen tai tt do

la mot bo cac quy trinh, cong cu, chinh sach can thiet de ngan chan viec truy cap trai phep, su dung, tiet lo, gian doan, sua doi va pha huy thong tin

C.I.A:

confidentility: tinh bao mat

integrity: tinh toan ven

availablility: tinh san co

He thong thong tin

con nguoi, phan cung, phan mem, thu tuc, du lieu, mang

Yeu cau cho cac he thong tt luon luon thay doi vi cac yeu to nguy co luon phat sinh bien doi, su can bang giua tinh bao mat va kha nang truy cap

**Chuc nang bao mat thong tin**

-bao ve kha nang hoat dong cua to chuc

-cho phep van hanh an toan cac ung dung tren to chuc cac he thong cntt

-bao ve du lieu ma to chuc thu thap va su dung

-bao ve cac tai san cong nghe ma to chuc su dung