QUIZ 1

Câu 1: Yêu cầu đối với một hệ thống thông tin an toàn?

Đảm bảo các thuộc tính C, I, A.

Một hệ thống thông tin an toàn cần đảm bảo 3 thuộc tính: Confidentiality (bí mật), Integrity (toàn vẹn) và Availability (sẵn sàng).

Câu 2: Giải thích các khái niệm Threat, Threat agent, Attack, Vulnerability và Risk trong an toàn thông tin.

Threat: Mối đe dọa đối với an ninh hệ thống.

Threat Agent: Tác nhân thực hiện tấn công

Attack: Quá trình thực hiện

Vulnerability: Lỗ hổng trong an ninh hệ thống

Risk: Thiệt hại của tổ chức khi tấn công xảy ra

1. Threat (sự đe dọa): mối đe doạ có thể tấn công hệ thống.

2. Threat agent (tác nhân đe dọa): con người hoặc phương tiện có khả năng gây hại hệ thống.

3. Vulnerability (lỗ hổng): điểm yếu trong bảo mật hệ thống có thể bị kẻ tấn công khai thác để phá hoại hệ thống.

4. Attack (tấn công): là các hành động tác nhân đe doạ khai thác lỗ hổng và khả năng bảo mật của hệ thống để truy cập trái phép, ăn cắp cơ sở dữ liệu, phá hoại, vô hiệu hoá, sửa đổi hệ thống... làm hệ thống tê liệt, hư hại hoặc mất mát dữ liệu.

5. Rick (nguy cơ, rủi ro): khả năng mối đe doạ tấn công và gây thiệt hại hệ thống.

Câu 3: X.800 là gì?

Mô hình an ninh tích hợp trong hệ thống mở (OSI). Mô tả Security Attacks, Security Mechanisms và Security Services.

X.800 là kiến trúc an ninh dùng cho OSI, được chuẩn hoá bởi ITU_T. Bao gồm: security attack, security mechanism, security service.

Câu 4: Security policy là gì? Ý nghĩa của nó trong an toàn thông tin?

Quy định của tổ chức sở hữu HTTT để đảm bảo khai thác HTTT an toàn.

1. Security policy là những quy định, chính sách của công ty, tổ chức giúp cho họ và những gì gắn liền với họ được an toàn.

2. Ý nghĩa trong an toàn thông tin: giúp cho nhân viên thực hiện theo những định hướng đã có nhằm mục đích đảm bảo an toàn cho hệ thống cùng với dữ liệu trước những nguy cơ bị xâm phạm.

Câu 5: Các ứng dụng của mật mã trong an toàn thông tin?

Đảm bảo C và I

Bảo mật thông tin.

- Mật mã đối xứng
- Mật mã bất đối xứng

Xác thực thông tin.

- Hàm băm
- Chữ ký số

Câu 6: Cơ chế hoạt động của mật mã đối xứng? Đặc điểm chung của các thuật toán mật mã đối xứng?

-Dùng chung khóa cho mã hóa và giải mã

-Đặc điểm chung: dựa trên các thao tác xử lý bit nên tốc độ mã hóa cao

1. Cơ chế hoạt động: thông tin gốc sau khi được mã hoá bằng thuật toán mã hoá cùng với khoá mật mã K sẽ được người gửi gửi cho người nhận. Người nhận sẽ dùng khoá mật mã K và thuật toán giải mã để giải mã thông tin đó cho ra thông tin gốc. Khoá mật mã K sẽ được dùng chung cho cả mã hoá và giải mã và được người gửi, người nhận trao đổi bí mật với nhau.

2. Đặc điểm chung: tốc độ nhanh, kích thước khối không thay đổi được (với DES là 64bit, AES là 128bit), khoá phải trao đổi bí mật.

Câu 7: Các thông số kỹ thuật của thuật toán DES? Điểm yếu của DES hiện nay là gì?

-Thông số: block size, key size, round number, operations

-Điểm yếu: khóa không đủ dài

1. Các thông số: chiều dài khoá, kích thước khối.

2. Điểm yếu của DES hiện nay: chiều dài khoá ngắn (56 bit) dẫn đến có thể bị bẻ khoá (bằng tấn công Brute-force)

Câu 8: Các thông số kỹ thuật của thuật tóan AES? AES có gì hay so với DES?

-Thông số: block size, key size, round number, operations

-Hay: tích hợp sẵn trong các bộ xử lý hiện đại -> chạy nhanh hơn

1. Các thông số: chiều dài khoá, kích thước khối.

2. So với DES thì AES: có kích thước khoá dài và có thể tuỳ chọn (128bit,192bit,256bit) .

Câu 9: Độ phức tạp của bài toán dò khóa (brute-force) một thuật toán mật mã là gì? Cách xác định?

-Độ phức tạp = thời gian

-Xác định: tốc độ dò * Tổng số khóa *1/2

Cách xác định?

1. Độ phức tạp của bài toán dò khóa (brute-force) một thuật toán mật mã là: thời gian để phá mã thuật toán.

2. Cách xác định: T = 2^(n-1)/t

T: thời gian thực hiện

n: chiều dài khoá

t: số khoá được dò trên 1 đơn vị thời gian

Câu 10: Các thành phần của một hệ thống mật mã đối xứng? Phần nào bí mật, phần nào công khai?

-Encryption algorithm, Decryption algorithm, key

-Bí mật: Key

1. Các thành phần: khoá mật mã, thông tin gốc, thông tin đã được mã hoá, thuật toán mã hoá, thuật toán giải mã. 2. Thông tin gốc và khoá mật mã được giữ bí mật, thông tin mã hoá được công khai.

QUIZ 2

Câu 1: Các ứng dụng của mật mã bất đối xứng trong an ninh thông tin?

-Mã hóa dữ liệu

-Xác thực dữ liệu

-Trao đổi khóa

Mật mã bất đối xứng trong an toàn thông tin giúp: bảo mật thông tin (Encrytion), xác thực thông tin (Authentication), trao đổi khoá trong mật mã đối xứng (Key exchange).

Câu 2: Với 3 thành phần: mật mã đối xứng, mật mã bất đối xứng và hàm băm, có thể thực hiện một giao dịch truyền thông tin an toàn giữa hai thực thể trên mạng hay không? Nếu có thì mô tả cơ chế thực hiện, nếu không thì cho biết còn yêu cầu nào chưa đáp ứng được?

-Không: mã đối xứng và bất đối xứng đảm bảo tính C, hàm băm chỉ đảm bảo một phần của tính I (toàn vẹn nội dung)

-Có: kết hợp giữa hàm băm với mật mã bất đối xứng để xác thực nguồn gốc

1. Chúng ta có thể thực hiện một giao dịch truyền thông tin an toàn giữa hai thực thể trên mạng với 3 thành phần nêu trên.

2. Cơ chế: các bên sẽ dùng mã hoá bất đối xứng để trao đổi khoá công khai với nhau, sau khi trao đổi khoá thành công các bên sẽ dùng mã hoá đối xứng trong việc trao đổi thông tin (mã hoá và giải mã thông tin) và sau cùng là dùng hàm băm để xác định tính toàn vẹn của thông tin trong quá trình truyền đi.

Câu 3: Public-key certificate là gì? Dùng để làm gì? Thành phần cơ bản của một public-key certificate?

-Chứng chỉ khóa công khai, dùng để chứng nhận sở hữu khóa công khai

-3 thành phần: Subject, public key, Digital signature

Public-key certificate: chứng thực khoá công khai, chứng chỉ số. Là một tài liệu điện tử dùng để chứng minh người sở hữu khoá công khai. Được dùng để xác nhận trong quá trình trao đổi khoá trong mật mã bất đối xứng.

Thành phần cơ bản của public-key certificate: khoá công khai, thông tin của người sở hữu, chữ kí số của nhà cung cấp chứng minh chứng chỉ số.

Câu 4: Mô tả trình tự các bước diễn ra trong một giao dịch điển hình giữa hai thực thể có dùng công cụ mật mã (gợi ý: tham khảo thủ tục bắt tay của giao thức SSL).

-A->B: Public key

-B->A: khóa K được mã hóa bằng Public key

-B<->A: Dữ liệu mã hóa bằng khóa K

1. Hai thực thể trao đổi thông tin của thuật toán mã hoá, và một số thông tin khác với nhau để nhận diện nhau.

2. Hai thực thể tiến hành xác thực thông tin của bên gửi, nếu một trong các bên không được xác thực thì giao dịch sẽ bị huỷ.

3. Sau khi xác thực thành công, hai bên sẽ tạo khoá để mã hoá và giải mã các thông tin trong phiên làm việc.

Câu 5: Mục đích của quản lý truy xuất (access control)? Liệt kê các công việc điển hình trong quy trình quản lý truy xuất của hệ thống thông tin?

-Mục đích: đảm bảo mỗi Subject chỉ thực hiện được các thao tác được phép

-Công việc: xây dựng chính sách, định danh, xác thực, cấp quyền, giám sát

Mục đích của quản lý truy xuất (access control): phân biệt truy xuất hợp lệ hay không. Bảo vệ tài nguyên khỏi các truy cập trái phép.

Các công việc điển hình trong access control: xây dựng chính sách, xác thực người dùng, cấp quyền truy cập.

Câu 6: Cơ sở của xác thực (authentication) là gì? Mục tiêu của xác thực?

-4 cơ sở: you know, you have, you are, you do

-Mục tiêu: kiểm tra định danh có đúng với subject hiện hành không

Cơ sở xác thực: bạn biết gì, bạn có gì, bạn là ai, bạn làm gì.

Mục tiêu xác thực: xác định người dùng quyền truy cập vào tài nguyên nào của hệ thống, giúp hệ thống đảm bảo được tính bí mật, toàn vẹn.

Câu 7: Liệt các kỹ thuật tấn công đối với cơ chế xác thực bằng password. Giải pháp đối phó với từng kỹ thuật tấn công là gì?

-Liệt kê các kỹ thuật tấn công trang 79/textbook

1.Offline dictionary attack: tấn công từ điển ngoại tuyến. Giải pháp: ngăn truy cập trái phép vào file mật khẩu, có biện pháp để phát hiện việc thay đổi mật khẩu có phù hợp hay không.

2.Specific account attack: tấn công tài khoản cụ thể. Giải pháp: khoá tài khoản sau một số lần đăng nhập thất bại.

3.Popular password attack: tấn công mật khẩu phổ biến. Giải pháp: hạn chế cho người dùng đặt mật khẩu dễ đoán.

4.Password guessing against single user: đoán mật khẩu đối với người dùng duy nhất. Giải pháp: quy định thời để thay đổi mật khẩu, quy định độ dài tối thiểu của một mật khẩu, hạn chế sử dụng thông tin cá nhân làm mật khẩu, cấm sử dụng tên những người nổi tiếng, các từ dễ đoán làm mật khẩu.

5.Workstation hijacking: tấn công máy trạm. Giải pháp: đăng nhập sau một thời gian không hoạt động.

6.Exploiting user mistakes: khai thác lỗi người dùng. Giải pháp: triển khai các biện pháp giúp người dùng phát hiện truy cập trái phép, bổ sung các cơ chế xác thực cho hệ thống.

7.Exploiting multiple password use: khai thác sử dụng mật khẩu nhiều lần. Giải pháp: đưa ra các chính sách để cấm hoặc hạn chế dùng 1 mật khẩu cho nhiều thiết bị mạng cụ thể.

8.Electronic monitoring: giám sát điện tử. Giải pháp: cần có biện pháp mã hoá mạnh hơn trong việc đăng nhập hoặc điều khiển từ xa.

Câu 8: Cách lưu trữ password của người dùng trong các hệ thống thông tin? Vai trò sủa salt trong lưu trữ password?

-Xử lý password trước khi lưu: mã hóa hoặc dùng hàm băm

-Salt làm tăng độ phức tạp (tăng số lần băm) của bài toán dò mật khẩu

1.Cách lưu: mật khẩu của người dùng sau khi được trộn thêm muối sẽ được băm chậm qua 1 hàm băm và lưu vào file. File này chứa: ID người dùng, muối và mã băm cho từng người dùng.

2.Vai trò của salt: giúp tạo ra một mật khẩu mạnh hơn, hacker khó khăn hơn trong việc tấn công.

Câu 9: Giải thích ý nghĩa của chính sách bảo mật sau đây trong Windows: "Accounts: Limit local account use of blank passwords to console logon only". Hãy cho một tình huống thực tế trong đó chính sách này nên được bật và một tình huống trong đó chính sách này nên được tắt.

-User có password trống không được truy xuất máy tính khác qua mạng

1. Ý nghĩa chính sách: giúp máy tính người dùng có thể đăng nhập từ xa mà không bị gián đoạn. Vì nếu tất cả tài khoản người dùng đếu được kích hoạt tính năng này thì không ai có thể đăng nhập thông qua dịch vụ đầu cuối.

2. Ví dụ:

Câu 10: Giải thích quyền "Increase a process working set" trong chính sách bảo mật của Windows. Mặc định thì những Subject nào trong hệ thống có quyền này. Cho biết chính sách này thuộc mô hình nào của quản lý truy xuất: DAC, MAC hay RBAC?

-Tăng kích thước vùng nhớ cấp phát cho tiến trình

-Thuộc mô hình quản lý MAC

1. Increase a process working set là quyền cho phép người dùng tăng kích thước vùng nhớ cho tiến trình làm việc.

2. Mặc định thì user có quyền này.

3. Chính sách này thuộc mô hình quản lý: DAC.

QUIZ 3

Câu 1: Liệt kê các cơ chế lây lan phổ biến của các phần mềm phá hoại máy tính. Kể tên các loại phần mềm phá hoại ứng với từng cơ chế lây lan.

-Lây qua thao tác sao chép (ký sinh vào file chủ)

-Tự lây lan qua mạng

-Lây lan bằng cách đánh lừa người dùng

1. Adware: quảng cáo được tích hợp vào trong phần mềm. Nó có thể dẫn đến pop-up quảng cáo hoặc là chuyển tiếp trình duyệt đến trang buôn bán nào đó.

2. Attack kits: bộ các công cụ để tự động tạo ra phần mềm độc hại mới bằng cách sử dụng nhiều cấp độ lây lan và các cơ chế cốt lõi.

3. Auto-rooter: những công cụ hacker xấu sử dụng để xâm nhập vào máy mới từ xa

4. Backdoor: bất kì cơ chế nào để tránh kiểm tra an ninh thông thường; nó có thể cho phép truy cập trái phép vào chức năng trong một chương trình, hoặc trên hệ thống bị tổn thương.

5. Exploits: mã cụ thể cho một lỗ hổng duy nhất, hoặc thiết lập các lỗ hổng

6. Flooders: được sử dụng để tạo ra một lượng lớn dữ liệu để tấn công các hệ thống mạng máy tính nối mạng, bằng cách tiến hành một số hình thức tấn công từ chối dịch vụ.

7. Keyloggers: ghi lại quá trình gõ phím trên hệ thống bị xâm nhập.

8. Logic bomb: mã được chèn vào phần mềm phá hoại bởi một kẻ xâm nhập. Một bom logic nằm im cho đến khi một điều kiện xác định được đáp ứng; đoạn mã sau đó sẽ gây ra hành động trái phép.

9. Macro virus: một loại virus sử dụng macro hoặc mã kịch bản, thường được nhúng trong một tài liệu, và kích hoạt khi tài liệu được xem hoặc được chỉnh sửa, để chạy và tái tạo chính nó vào các tài liệu tương tự khác.

10. Mobile code: phần mềm (ví dụ: ngôn ngữ kịch bản, đoạn chương trình, hoặc hướng dẫn cầm tay) mà nó có thể được vận hành không đổi cho những nền tảng khác nhau và thực thi chúng một cách giống nhau.

11. Rootkit: bộ công cụ hacker sử dụng sau khi kẻ tấn công xâm nhập vào trong hệ thống máy tính và đạt được quyền truy cập ở mức độ gốc.

12. Spammer: gửi một lượng lớn các e-mail, tin nhắn không cần thiết.

13. Spyware: phần mềm thu thập thông tin của một máy tính và truyền nó đến một hệ thống khác thông qua việc giám sát việc gõ phím, dữ liệu màn hình, và/hoặc lưu lượng truy cập mạng; hoặc là quét các tập tin có thông tin nhạy cảm trên hệ thống.

14. Trojan horse: chương trình máy tính được tung ra có chức năng hữu ích, nhưng nó cũng che giấu và tiềm ẩn các chức năng phần mềm phá hoại để tránh các coe chế bảo mật, đôi khi lợi dụng các huỷ quyền họp pháp của các phần của hệ thống để gọi chương trình trojan.

15. Virus: phần mềm phá hoại, khi được thực thi, nó cố gắng tự nhân bản chính nó vào trong máy khác có thể thực hiện được hoặc mã kịch bản; khi nó thành công, các mã được cho là bị nhiễm độc. Khi mã bị nhiễm độc được kích hoạt, virus cũng được kích hoạt.

16. Worm: một chương trình máy tính có thể chạy độc lập, có thể lan truyền trọn vẹn phiên bản thực thi của chính nó trên máy chủ khác trên mạng, thường là khai thác lỗ hổng của phần mềm trong hệ thống đích.

17. Zombie, bot: chương trình được kích hoạt trên máy bị nhiễm độc nó sẽ được kích hoạt để khởi động các cuộc tấn công trên các máy khác.

Những cơ chế lây lan phổ biến:

- Infected Content - Lây nhiễm vào nội dung (Sự lây nhiễm thực thi tại thời điểm đó hoặc nội dung được thực hiện bởi virus sau đó lan truyền đến các hệ thống khác): virus, macro virus.

- Vulnerability Exploit - Khai thác lỗ hổng phần mềm (Lợi dụng lỗ hổng của phần mềm kể cả cục bộ hoặc thông qua mạng bằng các loại sâu(worm) hoặc cố gắng tải xuống để cho phép phần mềm phá hoại nhân bản): worms, mobile code, backdoors.

- Social Engineering - Lừa đảo qua mạng (Kỹ thuật tấn công lừa đảo qua mạng làm cho người dùng tin tưởng nhằm tránh các cơ chế an ninh để cài đặt trojan, hoặc để phản hồi với các cuộc tấn công lừa đảo): spammer, trojan

Câu 2: Payload của phần mềm phá hoại là gì? Liệt kê một số loại payload phổ biến và các loại phần mềm phá hoại ứng với từng loại payload.

-Payload: tác động của phần mềm phá hoại lên hệ thống bit nhiễm.

-Các loại payload: system corruption, attack agent, information theft, stealthing

1. Trong phần mềm phá hoại, Payload là hành vi, phần cốt lõi của chương trình.

2. Các loại payload phổ biến:

- System Corruption (Phá vỡ hệ thống): logic bomb

- Attack Agent (Tác nhân tấn công): zombie, bots

- Attack Agent (Đánh cắp thông tin): keyloggers, spyware

- Stealthing (Lén lút, tự che giấu): backdoors, rootkits

Câu 3: So sánh cơ chế hoạt động của virus và worm.

-Virus: ký sinh trên file chủ, phát tán qua sao chép

-Worm: tự tồn tại, phát tán qua mạng

1.Giống nhau: Đều có thể tự nhân bản, Lây lan qua mạng, qua các phương tiện chia sẻ dữ liệu (CD, USB...)

2. Khác nhau: Virus lây lan được nhờ có sự tác động của con người. Cần có vật chủ để ký sinh (file thực thi, file tài liệu, boot sector...), Worm tự lây lan mà không cần bất kỳ sự tác tương nào. Worm có thể chạy một cách độc lập. Thường khai thác lỗ hổng của phần mềm.

Câu 4: Trình bày các điểm đặc trưng của từng loại phần mềm phá hoại: bots, spyware, rootkits.

-Bot: bị điều khiển bởi hệ thống từ xa

-Spyware: lấy cắp thông tin

-Rootkits: xâm nhập vào nhân hệ điều hành

1. Bots: khó theo dõi được hướng tấn công. Chỉ cần 1 máy kích hoạt sẽ khởi động các cuộc tấn công trên các máy khác với quy mô lớn. Điều khiển từ xa bởi ít nhất 1 máy.

2. Spyware: nội dung nhắm đến thường là mật khẩu, tài khoản của người dùng.

3. Rootkits: cố gắng ẩn nấp ẩn nấp đến mức tối đa và truy cập hệ thống với quyền quản trị cao nhất.

Câu 5: Các giải pháp đối phó với phần mềm phá hoại là gì?

-Prevention

-Detection

- Đảm bảo hệ thống được cập nhật các bản vá lỗi ứng dụng mới nhất để hạn chế số lỗi hacker có thể khai thác.

- Thiết lập quyền truy cập thích hợp vào các ứng dụng, dữ liệu lưu trên hệ thống nhằm hạn chế việc bất kì ai cũng có thể truy cập vào tệp tin, qua đó giảm nguy cơ hệ thống bị lây nhiễm phần mềm độc hại.

- Nâng cao nhận thức của người dùng nhằm tránh những lừa đảo qua mạng, đào tạo đội ngũ kỹ thuật tốt giúp hệ thống hạn chế bị lây nhiễm phần mềm phá hoại, khắc phục nhanh chóng khi bị lây nhiễm.

- Kiểm tra hệ thống thường xuyên để phát hiện sự bất thường.

- Sử dụng các giải pháp chuyên môn:

+ Phát hiện: nhận biết được hệ thống đã bị nhiễm và xác định vị trí của phần mềm phá hoại.

+ Nhận dạng: sau khi phát hiện ra cần nhanh chóng xác định chi tiết loại phần mềm phá hoại mà hệ thống bị nhiễm.

+ Loại bỏ: một khi đã nhận dạng chi tiết được loại phần mềm phá hoại, loại bỏ tất cả dấu vết của phần mềm phá hoại trên tất cả hệ thống bị nhiễm để nó không thể lay lan thêm nữa.

Câu 6: Mục tiêu tấn công của DoS là gì? Trình bày các kỹ thuật tấn công DoS truyền thống.

-Mục tiêu: chiếm dụng băng thông, chiếm dụng tài nguyên hệ thống, chiếm dụng tài nguyên ứng dụng

-Các kỹ thuật tấn công DoS truyền thống: ICMP flooding, SYN flooding, Source address spoofing

1. Mục tiêu: băng thông, tài nguyên hệ thống, tài nguyên ứng dụng

2. Các kỹ thuật tấn công DoS truyền thống:

- Dùng mô hình 1-1: dùng một máy mạnh ping đến máy yếu cho đến khi tê liệt

- ICMP flooding: khi nhận gói tin ICMP echo request (ICMP gửi lại yêu cầu), server sẽ gửi lại yêu cầu cho người gửi. Do đó kẻ tấn công gửi số lượng lớn gói tin nay đến server sẽ làm cho server bị tê liệt.

- Source address spoofing (giả mạo địa chỉ nguồn): kẻ tấn công giả mạo địa chỉ nguồn có đủ quyền truy cập vào mạng bình thường sau đó tạo ra lượng lớn gói tin gửi yêu cầu đến server.

- SYN flooding: kẻ tấn công khai thác lỗ hổng trong thủ tục bắt tay 3 chiều của TCP. Kẻ tấn công gửi một lượng rất lớn các kết nối giả mạo đến hệ thống đích, do địa chỉ máy đó không tồn tại nên khi server sẽ gửi gói tin SYN-ACK để xác nhận sẽ không nhận được phản hồi và server phải gửi lại gói SYN-ACK cho đến khi nhận được phản hồi...Do đó server sẽ bị nghẽn.

Câu 7: Flooding attack là gì, mục đích của flooding attack? Những kỹ thuật flooding attack phổ biến và đặc điểm của từng kỹ thuật.

-Flooding: chiếm dụng băng thông/tài nguyên hệ thống bằng cách gởi nhiều gói dữ liệu

-Những kỹ thuật flooding: ICMP flooding, UDP flooding, SYN flooding

1. Flooding attack (tấn công tràn ngập, ào ạt, tới tấp): trong mọi trường hợp ý định nói chung là làm quá tải dung lượng mạng trên một số liên kết đến một server. Cuộc tấn công có thể có các cách khác để làm quá tải khả năng xử lý, phản hồi của hệ thống.

Mục đích:

2. Các kỹ thuật flooding attack phổ biến:

- ICMP flooding: sử dụng những gói tin ICMP echo request (ICMP gửi lại yêu cầu) mà một số tường lửa cho gói này đi qua.

- UDP flooding: sử dụng những gói tin UDP.

- TCP SYN flooding: gửi yêu cầu kết nối TCP bình thường với một trong hai địa chỉ nguồn là thật hoặc giả mạo với số lượng lớn. Cũng có thể sử dụng gói dữ liệu TCP sẽ bị hệ thống từ chối vì nó không thuộc bất kỳ kết nối nào được biết đến, nhưng khoảng thời gian đó tấn công đã thành công trong việc làm tràn ngập các liên kết đến server.

Câu 8: Application-based bandwidth attack là gì? Cho ví dụ về loại tấn công này.

-Vét cạn tài nguyên ứng dụng

-Ví dụ: HTTP flooding, SIP flooding

1. Application-based bandwidth attack (tấn công băng thông ứng dụng, chiếm băng thông ứng dụng): cố gắng tận dụng lợi thế của một lượng lớn các tài nguyên không sử dụng tại một server.

2. Ví dụ: websites có thể làm các phép tính dài dòng chẳng hạn như nhiều tìm kiếm, trong việc trả lời một yêu cầu đơn giản.

Câu 9: Các giải pháp bảo vệ hệ thống khỏi tấn công DoS/DDdoS?

-Attack prevention and preemption

-Attack detection and filtering

-Attack source traceback and identification

-Attack reaction

- Attack prevention and preemption (ngăn ngừa và ngăn chặn trước các tấn công): quản lý raw packet interface, cơ chế dự phòng...

- Attack detection and filtering (tìm và lọc các tấn công): phát hiện dựa trên các mô tả trước

- Attack source traceback and identification (lần theo dấu vết và nhận diện nguồn tấn công)

- Attack reaction (phản ứng với tấn công): phối hợp với ISP

Câu 10: Khi hệ thống đang bị tấn công DoS/DdoS, người quản trị hệ thống cần thực hiện những thao tác gì để giảm thiểu thiệt hại?

-Nhận biết loại tấn công

-Phối hợp ISP để chặn lưu lượng tương ứng

- Nhận diện kiểu DoS/DDoS để tìm giải pháp tốt nhất đối phó lại nó.

- Phối hợp với ISP

- Nhờ đến sự trợ giúp của tổ chức chuyên nghiệp, cơ quan chức năng.

QUIZ 4

Câu 1: Trình bày tổ chức bộ nhớ của tiến trình. Khi tiến trình gọi 1 hàm có truyền đối số, thì đối số sẽ được lưu ở phần bộ nhớ nào của tiến trình?

-4 phần: Text, data, heap, stack

-Đối số chứa trong stack

1. Tổ chức bộ nhớ của chương trình

- Text: phần bộ nhớ chứa lệnh
- Data: phần chứa dữ liệu tĩnh
- Heap: phần chứa dữ liệu động
- Stack: phần chứa các biến thực thi chương trình, địa chỉ quay về

2. Khi tiến trình gọi 1 hàm có truyền đối số, thì đối số sẽ được lưu ở stack

Câu 2: Tấn công buffer overflow là gì? Nguồn gốc của tấn công này?

-Làm tràn vùng nhớ đã cấp phát

-Trình biên dịch không kiểm tra kích thước dữ liệu

1. Tấn công buffer overflow: kẻ tấn công lợi dụng lỗi buffer-overflow (tràn bộ nhớ đệm) để đưa dữ liệu đầu vào vượt quá kích thước cho phép của chương trình làm cho chương trình bị lỗi, treo... từ đó kẻ tấn công có thể chèn mã độc hoặc thực hiện các hành động phá hoại theo ý muốn.

2. Nguồn gốc

- Các chương trình không hoặc thực hiện thiếu đầy đủ trong việc kiểm tra kích thước dữ liệu đầu vào so với kích thước được cấp phép.
- Chương trình sử dụng các phương thức thiếu an toàn trong ngôn ngữ C như strcpy(), strcat(), gets()...vì những hàm này không kiểm tra kích thước dữ liệu được copy vào buffer.
- Chương trình được viết bằng ngôn ngữ C/C++, mà bản thân các ngôn ngữ này đã tiềm ẩn các lỗi mà hacker có thể khai thác.

Câu 3: Khi người dùng nhập dữ liệu có kích thước lớn hơn dung lượng vùng nhớ được cấp phát thì có những khả năng nào xảy ra?

-Không gây hại

-Tràn lên dữ liệu hệ thống

-Tràn lên dữ liệu người dùng

- Chương trình báo lỗi

- Dữ liệu bị tràn, ghi đè dữ liệu bên vùng nhớ khác

- Không có gì xảy ra

Câu 4: Shellcode là gì và có liên quan gì đến tấn công buffer overflow? Làm thế nào để tạo ra shellcode?

-Chương trình viết bằng mã máy

-Dùng để thực hiện thao tác mong muốn trên hệ thống bị tấn công

-Chuyển chương trình thực thi thành hợp ngữ, sau đó thành mã máy

1. Shellcode: một phần thiết yếu trong nhiều cuộc tấn công buffer-overflow là chuyển giao việc thực thi cho mã được cung cấp bởi kẻ tấn công và thường được lưu ở phần buffer bị tràn. Mã này được gọi là shellcode, bởi vì theo truyền thống chức năng kiểm soát chuyển giao được đưa tới người sử dụng trình thông dịch command-line, hoặc shell, nó cho phép truy cập bất kì chương trình nào có sẵn trên hệ thống với đặc quyền của chương trình kẻ tấn công. Shellcode sử dụng kết hợp với buffer-overflow cho phép thực thi thao tác bất kì trên hệ thống.

2. Một số ứng dụng giúp tạo shellcode: metasploit, shellcode framework...

Câu 5: Các giải pháp ngăn chặn tấn công buffer overflow?

-Compile-Time Defenses

-Run-Time Defenses

- Lựa chọn ngôn ngữ lập trình phù hợp

- Sử dụng các thư viện an toàn

- Chống tràn bộ đệm trên stack

- Bảo vệ không gian thực thi

- Ngẫu nhiên hóa sơ đồ không gian địa chỉ

- Kiểm tra sâu đối với gói tin

Câu 6: Mục đích của việc dùng công cụ IDA Pro khi thực hiện tấn công buffer overflow?

-Dịch ngược thì file thực thi thành hợp ngữ để tìm địa chỉ lệnh muốn thực thi

Công cụ IDA Pro giúp chuyển file thực thi về dạng mã cấp thấp assembly, qua đó hacker phân tích các lệnh trong chương trình muốn tấn công nhằm tìm ra lỗi beffer-overflow.

Câu 7: Mô tả vắn tắt CWE/SANS và OWASP top 10 (1 câu cho mỗi loại). Ý nghĩa hai khái niệm này trong software security?

-CWE: liệt kê 25 lỗi phần mềm phổ biến

A. CWE/SANS: một danh sách những loại phổ biến nhất của lỗi lập trình đã được khai thác trong nhiều cuộc tấn công lớn trước đó, chúng xảy ra thế nào và làm sao để tránh điều đó.
1. Insecure Interaction Between Components (Lỗi giao tiếp giữa các thành phần): Thất bại trong việc duy trì cấu trúc trang web ("Cross-site Scripting"). Thất bại trong việc duy trì cấu trúc truy vấn SQL ("SQL Injection"). Thất bại trong việc duy trì cấu trúc lệnh hệ điều hành ("OS Command Injection"). Giả mạo yêu cầu xuyên các trang (Cross-site) (CSRF). Tải lên không giới hạn các loại file nguy hiểm. Chuyển tiếp URL đến các trang không tin cậy ("Open Redirect")

2. Risky Resource Management (Lỗi quản lý tài nguyên): Sao chép buffer không kiểm tra kích thước của đầu vào ("Classic Buffer Overflow"). Tên đường dẫn giới hạn không thích hợp dẫn đến thư mục bị hạn chế ("Path Traversal"). Tải mã xuống mà không kiểm tra tính toàn vẹn. Chèn các hàm từ khu vực kiểm soát không tin cậy. Sử dụng hàm tiềm ẩn nguy hiểm. Tính toán sai kích thước của buffer. Không kiểm soát được định dạng chuỗi. Tràn hoặc quấn quanh (vòng tới) số nguyên.

3. Porous Defenses (Lỗi bảo vệ hệ thống): Thiếu xác thực cho các chức năng quan trọng. Thiếu(không) phân quyền. Sử dụng các chứng chỉ hard-coded. Quên mã hoá các dữ liệu nhạy cảm. Tin vào các đầu vào không tin cậy trong một quyết định an ninh. Thực thi với những đặc quyền không cần thiết. Phân quyền sai. Cho phép chuyển nhượng (phân quyền) sai tài nguyên quan trọng. Sử dụng thuật toán mã hoá bị hỏng hoặc nguy hiểm. Hạn chế không đúng (không hạn chế) những cố gắng xác thực quá mức. Sử dụng băm 1 chiều không có muối.

B. OWASP top 10
1. Injection (đưa vào, tiêm vào): dữ liệu không tin cậy được đưa đến trình thông dịch như 1 phần của câu lệnh hoặc câu truy vấn, kẻ tấn công lợi dụng để thực hiện lệnh không mong muốn hoặc truy cập dữ liệu mà không được phân quyền.

2. Broken Authentication and Session Management (quản lý phiên làm việc và xác thực bị hỏng): chức năng của ứng dụng liên quan đến xác thực và quản lý phiên thường không chính xác, kể tấn công lợi dụng để lấy mật khẩu, khoá... để mạo danh người dùng.

3. Cross-Site Scripting - XSS (kịch bản lệnh xuyên các trang): dữ liệu không đáng tin cậy được gửi đến trình duyệt web mà không cần hoặc trốn xác nhận, nó cho phép kẻ tấn công thực hiện các kịch bản trên trình duyệt nạn nhân như đánh cắp phiên làm việc, thay đổi nội dung trang web, chuyển hướng đến các trang độc hại.

4. Insecure Direct Object References (tham chiếu đối tượng trực tiếp không an toàn): nhà phát triển đưa ra một tham chiếu đến một đối tượng nội bộ như file, thư mục, CSDL khoá mà không cần kiểm soát hay sự bảo vệ khác. Kẻ tấn công tận dụng tham chiếu này để truy cập dữ liệu trái phép.

5. Security Misconfiguration (cấu hình sai an ninh): các thiết lập an ninh mặc định thường không an toàn, hệ thống bảo mật cần triển khai các phương pháp bảo mật cần thiết và có sự liên kết với nhau để tránh bị tấn công.

6. Sensitive Data Exposure (phơi bày dữ liệu nhạy cảm): các dữ liệu nhạy cảm không được bảo vệ đúng cách dẫn đến hậu quả nghiêm trọng khi bị tấn công.

7. Missing Function Level Access Control (thiếu kiểm soát truy cập chức truy cập các mức): hầu hết các ứng dụng web không kiểm tra sau khi xác minh quyền truy cập các cấp chức năng, kẻ tấn công lợi dụng để giả mạo người dùng để truy cập vào các chức năng mà không có quyền thích hợp.

8. Cross-Site Request Forgery (giả mạo yêu cầu xuyên trang): kẻ tấn công buộc trình duyệt của nạn nhân đăng nhập để gửi một yêu cầu http giả mạo...đến ứng dụng web có thể bị tấn công, điều này cho phép kẻ tấn công tạo ra các yêu cầu mà ứng dụng đó nghĩ là hợp pháp từ nạn nhân.

9. Using Components with Known Vulnerabilities (sử dụng các thành phần với lỗ hổng đã được biết đến): hầu như các thành phần trong ứng dụng luôn được chạy đủ quyền, nếu ứng dụng sử dụng các thành phần với các lỗ hổng đã được biết đến làm hệ thống phòng thủ suy yếu và dễ bị tấn công.

10. Unvalidated Redirects and Forwards (chuyển hướng và chuyển tiếp bất hợp lệ): các ứng dụng web chuyển hướng, chuyển tiếp không an toàn người dùng đến trang khác có thể bị kẻ tấn công lợi dụng để đưa nạn nhân đến các trang lừa đảo hoặc không được phép truy cập.

C. Ý nghĩa 2 khái niệm này trong software security:

- Giúp lập trình viên, kỹ thuật viên nắm bắt thông tin để tránh, khắc phục một số lỗi nguy hiểm, phát triển các ứng dụng an toàn

- Giúp các nhà phát triển biết và khắc phục lỗi của hệ thống do mình quản lý, bảo vệ hệ thống đúng cách, sử dụng các phần mềm an toàn

- Giúp người sử dụng có thêm kiến thức nhằm tránh các lỗi trong quá trình sử dụng có thể bị kẻ tấn công khai thác

Câu 8: Lỗi "Improper Neutralization of Input During Web Page Generation" trong liệt kê của CWE/SANS tương đương với lỗi gì trogn OWASP top 10 2013? Mô tả ngắn gọn cơ chế khai thác lỗi này.

XSS

1. "Improper Neutralization of Input During Web Page Generation" trong CWE/SANS tương đương với lỗi "Cross-Site Scripting" trong OWASP.

2. Kẻ tấn công đưa các đoạn mã độc vào trang web có lỗi XSS, ví dụ như chèn thêm đoạn script nguy hiểm vào url, bình luận...trong trang web, người dùng click vào thì các đoạn mã đó thực hiện theo kịch bản của kẻ tấn công nhằm đánh cắp thông tin, dữ liệu người dùng.

Câu 9: Mô hình tạo ra phần mềm an toàn gồm những bước nào?

Xử lý dữ liệu nhập

Viết mã nguồn an toàn

Đảm bảo an toàn khi tương tác với Hệ điều hành và các thành phần khác

Xử lý dữ liệu xuất

- Xử lý dữ liệu nhập

- Viết mã nguồn an toàn

- Đảm bảo an toàn khi tương tác với hệ điều hành và các thành phần khác

- Xử lý dữ liệu xuất

Câu 10: Mô tả cơ chế tấn công SQL injection. Cho ví dụ minh họa.

-Chèn câu truy vấn SQL vào form nhập liệu

1. Cơ chế tấn công SQL injection: 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 injection (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, thêm, sửa, xóa… trên cơ sở dữ liệu của ứng dụng.

2. Ví dụ: câu truy vấn SQL sau sẽ trả về tất cả các hàng từ bảng Users, với điều kiện luôn đúng là 1=1. Nếu bảng Users chứa tên và mật khẩu thì kẻ tấn công đánh cắp thông tin một cách dễ dàng.

```
SELECT * FROM Users WHERE UserId = 105 or 1=1
```

QUIZ 5

Câu 1: Tại sao firewall phải được cài đặt trên các thiết bị có ít nhất hai giao tiếp mạng?

-Để ép toàn bộ lưu lượng vào/ra phải qua firewall

Các mạng riêng nối với Internet thường bị đe dọa bởi những kẻ tấn công. Để bảo vệ dữ liệu bên trong người ta thường dùng firewall. Firewall có nhiệm vụ cho phép người dùng hợp lệ đi qua và chặn lại những người dùng không hợp lệ. Trong mọi trường hợp, nó phải được cài đặt trên thiết bị có ít nhất hai giao tiếp mạng, một cho mạng mà nó bảo vệ, một cho mạng bên ngoài.

Câu 2: So sánh cơ chế hoạt động của Packet Filtering firewall và Stateful Inspection firewall?

-Packet filtering: lọc từng gói độc lập

-Statefull inspection: kiểm tra theo trạng thái kết nối

1. Giống nhau: các quy tắc lọc dựa trên thông tin chứa trong gói network như: địa chỉ IP nguồn (Packet Filtering firewall),

địa chỉ IP đích (Packet Filtering firewall), địa chỉ tầng giao vận nguồn và đích (Source and destination transport-level address),

giao thức IP (IP protocol field), giao tiếp (Interface).

2. Khác nhau:

- Packet Filtering firewall: chỉ kiểm tra thông tin phần tiêu đề IP, không quan tâm đến trạng thái kết nối.

- Stateful Inspection firewall: ngoài việc kiểm tra thông tin của gói tin như Packet Filtering firewall, loại tường lửa này

còn ghi lại thông tin về các kết nối TCP, bảo vệ được các port cao của hệ thống, tránh backdoor.

Câu 3: Tấn công tiny fragments là gì?

-Phân mảnh cực nhỏ để vượt firewall

Những kẻ xâm nhập sử dụng tuỳ chọn phân mảnh IP để tạo ra những mảnh vô cùng nhỏ và cố gắng đưa thông tin tiêu đề TCP vào một gói các mảnh riêng biệt. Cuộc tấn công này được thiết kế để phá vỡ các quy tắc lọc mà nó (các quy tắc lọc) dựa vào thông tin tiêu đề TCP. Điển hình, một bộ lọc gói đưa ra quyết định lọc trên mảnh đầu tiên của một gói. Tất cả các mảnh tiếp theo của gói đó sẽ được lọc ra dựa trên cơ sở duy nhất đó là chúng (những mảnh tiếp theo) là một phần của gói tin mà mảnh đầu tiên đã bị loại bỏ. Những kẻ tấn công hy vọng rằng quá trình lọc tường lửa xem xét chỉ có mảnh đầu tiên và các mảnh còn lại được cho qua.

Câu 4: Tại sao Packet Filtering firewall không bảo vệ được các port cao của hệ thống?

-Khi tạo luận cho người dùng truy xuất ra ngoài thì phải mở tất cả các port cao theo chiều từ ngoài vào trong

Các port có số nhỏ hơn 1024 là những port được ấn định nhiệm vụ vĩnh viễn cho những ứng dụng riêng biệt, những port cao (từ 1024 đến 65535) được tạo ra tự động và mang tính chất tạm thời nên người quản trị không thể cài đặt hết chính sách cho những port đó, vì thế packet filtering firewall không thể bảo vệ các port cao của hệ thống.

Câu 5: Cho ví dụ về một luật truy xuất có thể thực hiện được bởi Application level firewall nhưng không thực hiện được bởi Network level firewall (kể cả packet filtering và stateful inspection)?

-Lọc nội dung truy xuất (hình ảnh, từ khóa, ...)

Network level firewall (kể cả packet filtering và stateful inspection)?

Ví dụ: luật truy xuất không cho người dùng xem hình ảnh/ chữ

- Source address: (internal) 192.168.1.106
- Destination address: (external) 210.9.88.29
- Source port: (>1023) 1030
- Destination port: 80
- Response: header content image/text
- Action: block

Câu 6: Chức năng của giao thức bảo mật SSL?

-Mã hóa

-Xác thực dữ liệu

-Xác thực đầu cuối

- Xác thực đầu cuối (peer authentication)
- Xác thực dữ liệu (data integrity)
- Mã hoá dữ liệu (data confidentiality)

Câu 7: Cơ chế xác thực đầu cuối của SSL được thực hiện như thế nào? Nếu muốn xác thực cả 2 phía đầu cuối (client và server) thì SSL sẽ thực thi như thế nào?

-Dùng certificate

-Cả 2 phía phải dùng certificate

- Client: trình duyệt sẽ sử dụng các kỹ thuật mã hoá công khai để kiểm tra Certificate và khóa công khai của server là có giá trị hay không và có được cấp bởi một CA đáng tin cậy hay không, rằng Certificate vẫn còn hiệu lực và Certificate đó có liên quan đến các trang web mà client liên lạc. Nếu server không được xác thực thì người sử dụng sẽ được cảnh báo và kết nối không được thiết lập. Ngược lại thì client sẽ thực hiện tiếp các bước sau đó.

- Server: phía server cũng sử dụng các kỹ thuật mã hoá công khai để kiểm tra xem chứng chỉ của phía client có giá trị hay không và có được cấp phát bởi một CA đáng tin cậy hay không. Trường hợp client không được xác thực, phiên làm việc sẽ bị ngắt. Còn nếu phía client được xác thực thành công, server sẽ thực hiện tiếp những công việc tiếp theo.

Câu 8: Vai trò của Certificate trong SSL?

-Xác thực đầu cuối và trao đổi khóa

Dùng để xác thực máy chủ có tin cậy hay không. Certificate cùng với khóa công khai đóng vai trò chứng thực rằng chắc chắn người dùng đang gửi thông tin trực tiếp đến ngay máy chủ và không gửi đến máy chủ của kẻ tấn công.

Câu 9: Kể tên các thao tác được thực hiện trên máy client khi nhận được certificate từ server?

-Kiểm tra subjetc

-Kiểm tra thời gian

-Kiểm tra chữ ký số

- Sử dụng thuật toán để kiểm tra certificate của server

- Gửi certificate của client cho server nếu được yêu cầu

- Gửi thông số trao đổi khoá (Client_key_exchage) cho server

- Có thể gửi xác minh certificate cho server

- Gửi cập nhật thông số mã (Change_cipher_spec) cho server

URL và dữ liệu HTTP đã được mã hóa.

Câu 10: Cơ chế tấn công man-in-the-middle đối với SSL?

-SSLstrip: chuyển từ HTTPS->HTTP

-SSLsplit: Ngắt kết nối thành 2 phần

Sử dụng các kỹ thuật khác nhau, kẻ tấn công chia tách các kết nối ban đầu thành 2 kết nối mới, một giữa client và những kẻ tấn công và một giữa những kẻ tấn công và server. Sau khi kết nối được chặn lại, những kẻ tấn công hoạt động như một proxy, có khả năng đọc, chèn và chỉnh sửa dữ liệu trong thông tin liên lạc bị chặn. Kẻ tấn công sẽ lấy các thông tin từ client gửi tới server (hoặc từ server đến client) và thực hiện ý đồ mà kẻ tấn công mong muốn trên thông tin lấy được, sau đó kẻ tấn công sẽ lấy thông tin đó và gửi lại cho server. Server và client vẫn tin rằng cả hai vẫn đang trực tiếp giao tiếp với nhau qua một kết nối riêng.