ĐỀ CƯƠNG ÔN TẬP

# Câu hỏi lý thuyết

* 1. Trình bày các hình thức tấn công? Nêu ví dụ minh họa? Liên hệ với các mục tiêu của an ninh mạng

<https://securitybox.vn/3126/top-6-hinh-thuc-tan-cong-mang-pho-bien-nhat/>

* + 1. Hình thức tấn công mạng bằng phần mềm độc hại (Malware Attack)

Một trong những hình thức tấn công mạng điển hình nhất những năm gần đây là hình thức tấn công bằng phần mềm độc hại (malware). Các phần mềm độc hại này bao gồm: mã độc tống tiền (ransomeware), phần mềm gián điệp (spyware), virus và worm (phần mềm độc hại có khả năng lây lan với tốc độ chóng mặt). Các tin tặc thường khai thác các lỗ hổng bảo mật để cài đặt malware nhằm xâm nhập và tấn công hệ thống.

Một số hậu quả do malware gây ra:

* Chặn người dùng truy cập vào các file hoặc folder nhất định
* Theo dõi hành động của người dùng và đánh cắp dữ liệu
* Làm hỏng phần cứng và làm ngưng trệ hoạt động
  + 1. Hình thức tấn công giả mạo (Phishing Attack)

Phishing Attack là hình thức tấn công trong đó tin tặc giả mạo thành một tổ chức hoặc cá nhân uy tín để lấy lòng tin của người dùng. Từ đó, chúng đánh cắp các dữ liệu nhạy cảm như tài khoản ngân hàng, thẻ tín dụng…

Các cuộc tấn công giả mạo thường được thực hiện qua email. Cụ thể, người dùng sẽ nhận được email giả mạo một tổ chức/ cá nhân uy tín với thông điệp vô cùng khẩn thiết. Thông điệp này yêu cầu người dùng click vào đường link tin tặc tạo ra. Nếu click vào, người dùng sẽ được chuyển đến một website giả mạo và được yêu cầu đăng nhập. Khi đó, tin tặc sẽ có được thông tin đăng nhập và dữ liệu nhạy cảm khác của người dùng.

Mục đích của tấn công Phishing thường là đánh cắp dữ liệu như thông tin thẻ tín dụng, mật khẩu. Đôi khi, tấn công phishing là để lừa người dùng cài đặt malware vào thiết bị. Lúc này, phishing là một công đoạn trong cuộc tấn công malware.

* + 1. Hình thức tấn công trung gian (Man in the middle attack)

Tấn công trung gian là hình thức tin tặc xen vào giữa phiên giao dịch hay giao tiếp giữa hai đối tượng. Khi đã xâm nhập thành công, chúng có thể theo dõi được mọi hành vi của người dùng. Tệ hơn, chúng có thể đánh cắp được toàn bộ dữ liệu trong phiên giao dịch đó. Tấn công trung gian dễ xảy ra khi nạn nhân truy cập vào một mạng wifi không an toàn.

* + 1. Hình thức tấn công từ chối dịch vụ (DoS & DDoS)

DoS (Denial of Service) là hình thức tấn công mà tin tặc đánh sập một hệ thống hoặc máy chủ tạm thời bằng cách tạo ra một lượng traffic khổng lồ ở cùng một thời điểm khiến cho hệ thống bị quá tải. Khi đó, người dùng không thể truy cập vào mạng trong thời gian tin tặc tấn công.

DDoS (Distributed Denial of Service) là hình thức biến thể của DoS. Theo đó, tin tặc sử dụng một mạng lưới các máy tính để tấn công. Sự nguy hiểm thể hiện ở chỗ chính các máy tính thuộc mạng lưới máy tính trên cũng không biết bản thân đang bị lợi dụng làm công cụ tấn công.

Hình thức tấn công DDoS chủ yếu nhắm vào các mục tiêu như: website, máy chủ trò chơi, máy chủ DNS… làm chậm, gián đoạn hoặc đánh sập hệ thống. Theo dự đoán của các cơ quan bảo mật, tần suất của tấn công DDoS sẽ ngày càng gia tăng. Nười dùng nên đặc biệt cẩn trọng.

* + 1. Hình thức tấn công cơ sở dữ liệu (SQL Injection)

SQL Injection là hình thức tấn công trong đó tin tặc chèn một đoạn mã độc hại vào server sử dụng ngôn ngữ SQL để đánh cắp những dữ liệu quan trọng.

Hậu quả lớn nhất của SQL Injection là làm lộ dữ liệu trong database. Đây là điều đặc biệt tối kỵ bởi chúng sẽ ảnh hưởng nặng nề đến uy tín của doanh nghiệp. Khi khách hàng mất niềm tin vào doanh nghiệp, khả năng cao họ sẽ sử dụng dịch vụ của bên khác. Doanh số giảm sút là hậu quả dễ thấy đầu tiên mà doanh nghiệp phải gánh chịu.

* + 1. Khai thác lỗ hổng Zero Day (Zero Day Attack)

Lỗ hổng Zero Day là các lỗ hổng bảo mật chưa được các nhà phát triển phần mềm biết tới. Vì vậy, chưa có bản vá chính thức cho các lỗ hổng này. Nói cách khác, các vụ tấn công Zero Day xảy ra một cách bất ngờ mà các nhà phát triển phần mềm không thể dự liệu trước. Đó là lý do hậu quả của các vụ tấn công Zero Day thường vô cùng nặng nề.

* 1. Trình bày các mục tiêu của an ninh mạng? Lấy ví dụ?
  2. Khái niệm mã hóa công khai? Sử dụng mã hóa công khai làm chữ ký số?
  3. Trình bày khái niệm firewall, cơ chế kiểm soát, ưu điểm và hạn chế?
  4. Khái niệm về các phần mềm độc hại, phân loại?
  5. Phân loại firewall? Trình bày về cơ chế Package Filtering?
  6. Nêu các hình thức tấn công? Liên hệ với các mục tiêu của an ninh mạng
  7. Trình bày về Circuit‐level Gateway trong firewall?
  8. Trình bày về các loại firewall topology?
  9. Khái niệm chữ ký số? Sử dụng mã hóa công khai thực hiện giao dịch có chữ ký số?
  10. Trình bày các bước để mã hóa theo thuật toán Caesar Cipher? Lấy ví dụ mã hóa một chuỗi ký tự tùy chọn để minh họa.
  11. Khi trao đổi thông điệp qua mạng tính toàn vẹn (integrity) được yêu cầu thế nào? Thực hiện yêu cầu toàn vẹn bằng giải pháp nào?
  12. Trình bày các bước để mã hóa theo thuật toán Vigenere Cipher? Lấy ví dụ mã hóa một chuỗi ký tự tùy chọn để minh họa.
  13. Nêu những hạn chế (nguy cơ bị bẻ khóa) của các phương pháp mã hóa kinh điển. Lấy ví dụ trong trường hợp Caesar Cipher và Vigenere Cipher
  14. Trên cơ sở phân tích các hạn chế của các thuật toán mã hóa cổ điển (Caesar Cipher, Vigeniar Cipher), các chuẩn mã hóa tiên tiến được thiết kế như thế nào? Trình bày các phép biến đổi cơ bản hay được sử dụng trong các chuẩn mã hóa tiên tiến.
  15. Nêu các hạn chế của firewall? Các cơ chế thiết lập firewall?
  16. Trình bày cách thiết lập một bộ khóa trong thuật toán RSA. Sử dụng bộ khóa đó để mã hóa và giải mã một ký tự tùy chọn
  17. Nêu những hiểu biết của bạn về hàm băm (Hash function) và sử dụng hàm băm trong đảm bảo tính toàn vẹn của thông điệp?
  18. Nêu kiến trúc các mô hình cài đặt firewall?
  19. Trình bày về SQL Injection và cách khắc phục

# Bài tập

## Sử dụng Java Cryptography Architecture (JCA), viết class SymmetricCryp để thực hiện các chức năng mã hóa và giải mã đối xứng theo thuật toán AES gồm các hàm

1.1 Sinh khóa đối xứng

1.2 Tạo khóa đối xứng từ một chuỗi cho trước

1.3 Mã hóa thông điệp có 2 tham số: Tham số 1 là chuỗi cần mã hóa, tham số thứ 2 là khóa được tạo ở 1.1

1.4 Mã hóa thông điệp có 2 tham số: Tham số 1 là chuỗi cần mã hóa tham số 2 là khóa được tạo ở 1.2

1.5 Giải mã có 2 tham số: Tham số 1 là bản mã, tham số thứ 2 là khóa bí mật được tạo ở 1.1

1.6 Giải mã có 2 tham số: Tham số 1 là bản mã, tham số thứ 2 là khóa bí mật được tạo ở 1.2

1.7 Sử dụng class SymetricCryp để mã hóa một chuỗi cho trước hoặc giải mã ra bản rõ từ bản mã cho trước.

## Sử dụng Java Cryptography Architecture (JCA) để viết các hàm băm thông điệp cho trước theo thuật toán:

2.1. MD5

2.2. SHA1

2.3. SHA-256

## Sử dụng Java Crypto Architecture (JCA), viết chương trình mã hóa và giải mã sử dụng mã hóa công khai RSA:

Viết class RSAKeyGen để sinh bộ khóa công khai gồm các hàm

3.1 Sinh bộ khóa theo thuật toán RSA

3.2 Lưu bộ khóa ra file

Viết class RSACryp để sử dụng bộ khóa đã lưu trong file để mã hóa và giải mã thông điệp theo thuật toán RSA

3.3 Hàm đọc file để nạp khóa bí mật, tham số truyền vào là tên file

3.4 Hàm đọc file để nạp khóa công khai, tham số truyền vào là tên file

3.5 Hàm mã hóa một thông điệp cho trước bằng khóa bí mật, tham số truyền vào gồm tham số thứ nhất là thông điệp cần mã hóa, tham số thứ 2 là khóa bí mật

3.6 Hàm giải mã thông điệp bằng khóa công khai, tham số truyền vào gồm tham số thứ nhất là bản mã cần giải mã, tham số thứ 2 là khóa công khai.

3.7 Sử dụng lớp RSACryp để mã hóa một chuỗi và băm chuỗi theo một thuật toán băm cho trước rồi lưu cả bản mã và bản băm vào một file

3.8 Đọc file chứa bản mã và bản băm của một thông điệp, sử dụng lớp RSACryp để giải mã ra thông điệp gốc và băm lại bằng thuật toán băm cho trước. Sau đó đem so sánh hai bản băm để xác nhận tính toàn vẹn

## Lập trình mô tả lỗi SQL Injection và cách khắc phục

## Các bài tập đã làm trên lớp và trong giờ thực hành