ĐỀ CƯƠNG ÔN TẬP

Phần 1: 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

* Các hình thức tấn công:
* Malware – tấn công bằng phần mềm độc hại
* Tấn công giả mạo
* Tấn công từ chối dịch vụ
* Tấn công trung gian
* Khai thác lỗ hổng zero – day
* Tấn công email
* Tấn công chuỗi cung ứng
* Tấn công vào con người
* Tấn công nội bộ tổ chức
* Ví dụ minh họa
* Liên hệ

1. Trình bày các mục tiêu của an ninh mạng? Lấy ví dụ?

* Trình bày các mục tiêu của an ninh mạng: bảo về thông tin khỏi bị đánh cắp, xâm phạm hoặc tấn công

1. Khái niệm mã hóa công khai? Sử dụng mã hóa công khai làm chữ ký số?
2. Trình bày khái niệm firewall, cơ chế kiểm soát, ưu điểm và hạn chế?
3. Khái niệm về các phần mềm độc hại, phân loại?
4. Phân loại firewall? Trình bày về cơ chế Package Filtering?
5. Nêu các hình thức tấn công? Liên hệ với các mục tiêu của an ninh mạng
6. Trình bày về Circuit‐level Gateway trong firewall?
7. Trình bày về các loại firewall topology?
8. Khái niệm chữ ký số? Sử dụng mã hóa công khai thực hiện giao dịch có chữ ký số?
9. 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.
10. 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?
11. 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.
12. 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
13. 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.
14. Nêu các hạn chế của firewall? Các cơ chế thiết lập firewall?
15. 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
16. 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?
17. Nêu kiến trúc các mô hình cài đặt firewall?
18. Trình bày về SQL Injection và cách khắc phục

Phần II: Bài tập

1. 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.

2. 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

3. 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

4. Lập trình mô tả lỗi SQL Injection và cách khắc phục

5. Mô tả một số ví dụ khai thác lỗi SQL Injection trên các bài CTF của Root-me.org:

- Input như thế nào để khai thác?

- Output khi đó ra sao? => đưa ra nhận định để khai thác bước tiếp theo.

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