**MỤC LỤC**

[1. Trình bày các hình thức tấn công? Nêu ví dụ minh họa? 3](#_Toc152674985)

[2. Trình bày các mục tiêu của an ninh mạng? Lấy ví dụ? 3](#_Toc152674986)

[3. Khái niệm mã hóa công khai? Sử dụng mã hóa công khai làm chữ ký số? 3](#_Toc152674987)

[4. Trình bày khái niệm firewall, cơ chế kiểm soát, ưu điểm và hạn chế? 4](#_Toc152674988)

[5. Khái niệm về các phần mềm độc hại, phân loại? 5](#_Toc152674989)

[6. Phân loại firewall? Trình bày về cơ chế Package Filtering? 5](#_Toc152674990)

[7. Trình bày về Circuit‐level Gateway trong firewall? 6](#_Toc152674991)

[8. Trình bày về các loại firewall topology? 6](#_Toc152674992)

[9. Khái niệm chữ ký số? Trình bày ứng dụng mã hóa công khai 7](#_Toc152674993)

[10. Trình bày các bước để mã hóa theo thuật toán Caesar Cipher? Lấy ví dụ mã hóa a. 7](#_Toc152674994)

[11. Khi trao đổi thông điệp qua mạng tính toàn vẹn (integrity) được yêu cầu thế nào? 8](#_Toc152674995)

[12. Trình bày các bước để mã hóa theo thuật toán Vigenere Cipher? Lấy ví dụ mã hóa 8](#_Toc152674997)

[13. Nêu những hạn chế (nguy cơ bị bẻ khóa) của các phương pháp mã hóa kinh điển. 9](#_Toc152674998)

[14. Trên cơ sở phân tích các hạn chế của các thuật toán mã hóa cổ điển. Trình bày các phép biến đổi cơ bản hay được sử dụng trong các chuẩn mã hóa tiên tiến. 9](#_Toc152674999)

[15. Nêu các hạn chế của firewall? Các cơ chế thiết lập firewall? 9](#_Toc152675000)

[16. Trình bày cách thiết lập một bộ khóa trong thuật toán RSA. 10](#_Toc152675001)

[17. Nêu những hiểu biết của bạn về hàm băm (Hash function) và sử dụng hàm băm 10](#_Toc152675002)

[18. Nêu kiến trúc các mô hình cài đặt firewall? 11](#_Toc152675003)

[19. Trình bày về SQL Injection? Nêu ví dụ và cách khắc phục 12](#_Toc152675004)

[20. Trình bày về Cross-Site Scripting (XSS)? Nêu ví dụ và cách khắc phục 12](#_Toc152675005)

[21. Trình bày về XML Injection? Nêu ví dụ và cách khắc phục 13](#_Toc152675006)

[22. Trình bày về Directory Traversal/Command Injection? 13](#_Toc152675007)

[23. Trình bày một số hình thức tấn công phía client: Header manipulation, Cookies 14](#_Toc152675008)

[24. Trình bày hình thức tấn công phía client: Attachments, Session Hijacking 15](#_Toc152675010)

[25. Trình bày về DoS và các loại tấn công DoS 15](#_Toc152675012)

[26. Trình bày về Interception, Poisioning và các hình thức tấn công chiếm quyền truy cập (Access Rights) 15](#_Toc152675013)

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

**-** Tấn công đánh chặn: nguồn tài nguyên không sẵn sàng bị chặn.

Ví dụ: A gửi cho B 1 gói tin bị chặn bởi C và gói tin đấy ko đến được tới B. Liên hệ: Availability

- Tấn công gián đoạn: dữ liệu được đọc bởi người ko có quyền. Đây là kiểu tấn công bảo mật. Ví dụ: A gửi cho B gói tin bị C xem nhưng gói tin vẫn đến được tới B. Liên hệ: Confidentiality

- Tấn công sửa đổi: dữ liệu được sủa đổi bởi người không có quyền. Đây là kiểu tấn công toàn vẹn dữ liệu.

Ví dụ: A gửi cho B 1 gói tin, C chặn gói tin sửa đổi nội dung rồi gửi gói tin đã bị chỉnh sửa đến B. Liên hệ: Integrity

- Tấn công giả mạo: Giả mạo người gửi.

Ví dụ: C giả mạo A gửi gói tin đến B. Liên hê: Message Origin Anthentication, Timeliness

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

Có 3 mục tiêu chủ yếu:

* Tính bảo mật. Ví dụ: A và B ko muốn thông điệp của họ bị đọc bởi người khác.
* Tính toàn vẹn. Ví dụ: A và B ko muốn thông điệp của họ bị thay đổi bởi người khác.
* Tính sẵn sàng. Ví dụ: Đảm bảo máy chủ B luôn nhận được yêu cầu hợp lệ.

Ngoài ra còn 6 mục tiêu nữa:

* Xác thực thực thể. Ví dụ: A muốn xác nhận thông điệp được gửi từ B chắc chắn từ B gửi.
* Xác thực nguồn gốc của thông điệp. Ví dụ: A muốn chắc chắn thông điệp được cho là gửi đến từ B là từ B gửi và ngược lại.
* Timeliness – tính kịp thời: Ví dụ: ngăn chặn bên thứ 3 sao chép nội dung cuộc trò chuyện
* Chống từ chối: Ví dụ: A ko thể nào từ chối được thông điệp của mình đã gửi và đã nhận.
* Cấp phép: Ví dụ: một máy tính trên mạng có tài nguyên sẵn sàng cho một tập người dùng, nhưng ko phải tất cả người dùng mạng có thể truy cập được nguồn tài nguyên này.
* Quyền truy cập: Ví dụ: giống như phân quyền trong DB

## 3. Khái niệm mã hóa công khai? Sử dụng mã hóa công khai làm chữ ký số?

Mã hóa khóa công khai là một dạng mã hoá cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai và khóa cá nhân (hay khóa bí mật).

Sử dụng mã công khai làm chữ ký số:

Bên A:

A muốn gửi thông điệp M và A sử dụng chữ ký số:

* A băm thông điệp M => 1 giá trị băm
* Giá trị băm dùng khoá private của A để mã hoá => chữ ký điện tử
* Đính kèm chữ ký điện tử với thông điệp M rồi gửi đến B.

Bên B:

* B gói tin của A gửi lấy ra thông điệp M và băm => giá trị băm (1)
* Lấy chữ ký mã hoá theo khoá public của A => giá trị băm (2)
* Nếu giá trị băm (1) bằng băm (2) thì chữ ký được xác thực và ngược lại.

## 4. Trình bày khái niệm firewall, cơ chế kiểm soát, ưu điểm và hạn chế?

**Firewall:**

Firewall là một hệ thống an ninh mạng được sử dụng để ngăn chặn và kiểm soát lưu lượng truy cập giữa mạng nội bộ và mạng bên ngoài, nhằm bảo vệ hệ thống và dữ liệu khỏi các mối đe dọa từ internet hoặc các mạng không an toàn. Firewalls có thể được triển khai ở cấp độ phần cứng hoặc phần mềm.

**Cơ chế kiểm soát:**

* Các cơ chế kiểm soát của firewall bao gồm:
* Kiểm soát Địa chỉ IP: Firewall có thể cấm hoặc cho phép truy cập dựa trên địa chỉ IP nguồn và đích.
* Kiểm soát Cổng: Firewall kiểm soát lưu lượng dựa trên số cổng mà nó đi qua. Mỗi dịch vụ trên mạng sử dụng một cổng cụ thể.
* Kiểm soát Ứng dụng: Một số firewall hiện đại có khả năng kiểm soát ứng dụng, ngăn chặn hoặc cho phép dựa trên loại ứng dụng sử dụng.
* Kiểm soát Nội dung: Firewall có thể kiểm soát nội dung dựa trên quy tắc được thiết lập trước, như chặn các trang web cụ thể hoặc từ khóa.

**Ưu điểm:**

* Bảo vệ an ninh mạng: Firewall ngăn chặn các mối đe dọa từ mạng ngoại vi, bảo vệ hệ thống và dữ liệu.
* Kiểm soát truy cập: Người quản trị có thể thiết lập các quy tắc để kiểm soát và giám sát việc truy cập mạng.
* Bảo vệ dữ liệu nhạy cảm: Firewall giúp ngăn chặn truy cập trái phép vào dữ liệu quan trọng.
* Ngăn chặn tấn công mạng: Firewall có thể phát hiện và ngăn chặn nhanh chóng các loại tấn công mạng.

**Hạn chế:**

* Khả năng chặn nhầm: Có thể xảy ra trường hợp firewall chặn truy cập hợp lý vì quy tắc cấu hình không chính xác.
* Khả năng vượt qua: Một số kỹ thuật tấn công có thể vượt qua firewall nếu chúng được thực hiện một cách thông minh.
* Chỉ bảo vệ ở mức mạng: Firewall tập trung chủ yếu vào việc bảo vệ ở mức mạng, trong khi mối đe dọa từ bên trong mạng (ví dụ như từ nhân viên) vẫn có thể xảy ra.
* Hiệu suất có thể bị ảnh hưởng: Việc kiểm soát mọi gói tin mạng có thể ảnh hưởng đến hiệu suất của mạng, đặc biệt là trong các môi trường có lưu lượng cao.
* Tóm lại, firewall là một phần quan trọng trong việc bảo vệ mạng và dữ liệu, nhưng cần được kết hợp với các biện pháp an ninh khác để đảm bảo mức độ bảo vệ toàn diện.

## 5. Khái niệm về các phần mềm độc hại, phân loại?

\* Phần mềm độc hại: là phần mềm xâm nhập vào hệ thống máy tính mà không có sự hiểu biết hoặc chấp thuận của người dùng và sau đó thực hiện hành động không mong muốn, thường có hại.

\* Phân loại các phần mềm độc hại:

**- Phụ thuộc vào chương trình chủ**:

+ Trapdoors: cài đặt một điểm truy cập trái phép cho phép người dùng khác truy cập vào máy tính mà không có sự đồng ý của bạn

+Logic Bombs: đoạn mã độc hại được kích hoạt khi gặp tình huống đặc biệt

+ Trojan Horses: ẩn mình dưới dạng chương trình hữu ích và có những chức năng người dùng cần, nhưng thực chất lại âm thầm thực hiện hành vi xấu, thậm chí cài đặt virus vào máy

+Viruses: tự sao chép bản thân nó vào các chương trình khác của hệ thống

**- Độc lập lây nhiễm**:

+ Bacteria: làm full ổ cứng, hoặc CPU

+ Worms: tự nhân bản trong hệ thống hoặc thậm chí lây từ máy tính này sang máy tính khác

## 6. Phân loại firewall? Trình bày về cơ chế Package Filtering?

Phân loại Firewall:

Có 3 loại firewall phổ biến

+ Packet-Filtering Firewall: là loại firewall phổ biến nhất

+ Circuit-level gateway: làm việc ở cấp độ phiên của mô hình lớp mạng OSI

+ Application-level gateway: thường được sử dụng cùng với Packet-Filtering Firewall.

Cơ chế Packet-Filtering Firewall:

+ Firewall sẽ áp dụng một tập các quy tắc cho mỗi gói tin IP đi đến và sau đó quyết định sẽ chuyển tiếp hay loại bỏ gói tin đó đi.

+ Bộ lọc gói thường được thiết lập bằng danh sách quy tắc dựa vào các trường header IP và TCP.

+ Có 2 chính sách mặc định: discard và forward

## 7. Trình bày về Circuit‐level Gateway trong firewall?

+ Làm việc ở tầng vận chuyển của mô hình OSI, hoặc nó ở tầng “shim-layer” giữa tầng ứng dụng và tầng vận chuyển của ngăn TCP/IP.

+ Nó kiểm soát cơ chế bắt tay của TCP giữa các gói tin để xác định liệu 1 phiên yêu cầu có hợp lệ hay không.

+ Là hệ thống tiêu chuẩn độc lập.

+ Cổng thường chuyển tiếp các TCP segment từ 1 kết nối đến một kết nối khác mà ko cần xem xét nội dung của nó.

+ Chức năng bảo mật bao gồm việc xác định những kết nối nào sẽ được cho phép

+ Dùng trong trường hợp người quản lý hệ thống tin tưởng những người dùng nội bộ.

## 8. Trình bày về các loại firewall topology?

Các loại firewall topology

* Simplest firewall topology: Đây là cấu trúc đơn giản nhất. Trong hầu hết các trường hợp, firewall là một packet filter firewall.
* Single Homed Host: Một Single Homed Host có một packet filter firewall với 1 cổng ứng dụng phía sau firewall. Cổng ứng dụng điều chỉnh quyền truy cập vào máy chủ thông tin. Nó cũng được sử dụng để điều chỉnh truy cập internet bởi các máy nội bộ. Máy chủ thông tin có thể được phép truy cập internet thông qua packet filter firewall, nhưng các thiết bị khác trên mạng nội bộ phải truy cập internet thông qua cổng ứng dụng.
* Dual Homed Bastion: Nó có 1 packet filter firewall với cổng ứng dụng phía sau firewall. Máy chủ lưu trữ điều chỉnh quyền truy cập vào máy chủ thông tin. Nó cũng được sử dụng để điều chỉnh truy cập vào internet bởi các máy tính cá nhân mạng nội bộ vì tất cả phải đi qua máy chủ mạng lưu trữ kép. Hệ thống này đảm bảo an ninh hơn vì ngay cả khi firewall bị xâm nhập, mạng nội bộ thì vẫn ẩn.
* DMZ: Có 1 packet filter firewall với cổng ứng dụng phía sau firewall. Có 1 packet filter firewall giữa cổng ứng dụng và mạng nội bộ. Khoảng cách giữa 2 packet filter firewall được gọi là DMZ. DMZ chứa tất cả các máy chủ có sẵn công khai của tổ chức. Đây là 1 cấu hình rất an toàn

## 9. Khái niệm chữ ký số? Trình bày ứng dụng mã hóa công khai để thực hiện giao dịch có chữ ký số?

\* Chữ ký số là thông tin đi kèm theo dữ liệu (văn bản: word, excel, pdf…; hình ảnh; video...) nhằm mục đích xác định người chủ của dữ liệu đó, có thể được cung cấp đến dịch vụ an ninh về toàn vẹn thông điệp.

\* Sử dụng mã hóa công khai thực hiện giao dịch có chữ ký số:

Bên A:

A muốn gửi thông điệp M và A sử dụng chữ ký số:

* A băm thông điệp M => 1 giá trị băm
* Giá trị băm dùng khoá private của A để mã hoá => chữ ký điện tử
* Đính kèm chữ ký điện tử với thông điệp M rồi gửi đến B.

Bên B:

* B gói tin của A gửi lấy ra thông điệp M và băm => giá trị băm (1)
* Lấy chữ ký mã hoá theo khoá public của A => giá trị băm (2)
* Nếu giá trị băm (1) bằng băm (2) thì chữ ký được xác thực và ngược lại.

## 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.

B1: xoá tất các ký tự đặc biệt nằm ngoài bảng chữ cái (ví dụ: số, dấu chấm, dấu phẩy, dấu nháy...) và chuyển chữ hoa thành chữ thường.

B2: Xác định 1 khoá là một số nằm trong khoảng từ 0 đến 25. Vẽ bảng thể hiện sự thay đổi của mỗi chữ cái.

B3: Chuyển đổi bản rõ thành bản mã.

Thêm VD:

mật mã caesar

Input: M = NOROSEWITHOUTATH

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Gốc: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|  | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| K=8 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |

Key: K = 8. Tìm Output: C =

**Giải:**

Input: M = NOROSEWITHOUTATH

C = VWZWAMEQBPWCBIBP

## 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?

## - Yêu cầu của tính toàn vẹn khi trao đổi thông điệp là đảm bảo thông điệp không bị sửa đổi bởi bất kỳ ai trong quá trình giao dịch.

Giải pháp:

- Hàm băm: là công cụ chính được sử dụng để cung cấp tính toàn vẹn

Có hai loại hàm băm:

+ Hàm băm không khóa: là những hàm băm không yêu cầu bất kì đầu vào nào ngoài thông điệp được băm

+ Hãm băm có khóa: là những hàm yêu cầu khóa cũng như thông điệp được băm

- Messeage Athentication Codes (MAC): là một đoạn thông tin ngắn được sử dụng để xác thực thư. Giá trị MAC bảo vệ cả tính toàn vẹn dữ liệu của tin nhắn cũng như tính xác thực của nó, bằng cách cho phép người xác minh (người cũng sở hữu khóa bí mật) phát hiện bất kỳ thay đổi nào đối với nội dung tin nhắn.

## 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.

- B1: xoá tất các ký tự đặc biệt nằm ngoài bảng chữ cái (ví dụ: số, dấu chấm, dấu phẩy, dấu nháy...) và chuyển chữ hoa thành chữ thường.

- B2: Chọn khoá là một từ.

- B3: Tìm thứ tự của từng ký tự trong khoá tương ứng với bảng chữ cái.

- B4: Ánh xạ bản rõ với ma trận Vigenere Square and Demonstration theo thứ tự của khoá trong bảng chữ cái được bản mã.

Thêm vd:

mật mã vigenere – lặp khóa

Input: M = MONEYMAKESTHE

Key: K = YOUREON

Tìm Output: C =

**Giải:**

M = MONEYMAKESTHE

K = YOUREONYOUREO

Tra bảng ta được:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | O | N | E | Y | M | A | K | E | S | T | H | E |
| Y | O | U | R | E | O | N | Y | O | U | R | E | O |
| K | C | H | V | C | A | N | I | S | M | K | L | S |

* C = KCHVCANISMKLS

## 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

**- Phương pháp mã hóa kinh điển** là kỹ thuật đơn giản nên phương pháp mã hóa dữ liệu này có tính an toàn không cao. Việc giữ bí mật thuật toán cũng chỉ đảm bảo ở mức tương đối, nếu trường hợp nó bị rò rỉ ra ngoài hoặc kẻ xấu có thể lần mò giải ra thuật toán thì việc mã hóa trở nên vô nghĩa.

- Ví dụ: Caesar và Vigenere đều dùng phương pháp thay thế 1 ý tự này bằng 1 ký tự khác trong bảng chữ cái nên không gian khóa chính là bảng chữ cái gồm 26 ký tự.

+ Với Caesar Cipher, có thể thử mò 26 vị trí thay đổi ký tự

+ Với Vigenere Cipher, nếu bị lộ từ khóa thì có thể dễ dàng giải mã ngược.

## 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.

- **Các chuẩn mã hóa tiên tiến** được thiết kế xoay quanh việc sử dụng “khóa bí mật” để mã hóa dữ liệu, áp dụng kích thước khóa lớn hơn, nhiều khóa hơn, đồng thời thực hiện mã hóa nhiều vòng để làm tăng tính bảo mật và đem lại độ an toàn.

- Phép biến đổi cơ bản hay được sử dụng trong các chuẩn mã hóa tiên tiến:

+ Thay thế

+ Dịch chuyển

+ Đổi chỗ

+ Đảo bit

+ Dịch vòng

+ Phép XOR bit

## 15. Nêu các hạn chế của firewall? Các cơ chế thiết lập firewall?

- Các hạn chế của firewall:

+ Firewall ko thể chống lại các cuộc tấn công ko đi qua nó.

+ Firewall ko thể chống lại các nguy cơ tấn công từ chính bên trong mạng nội bộ mà nó bảo vệ

+ Firewall ko thể bảo vệ chống lại việc chuyển các chương trình hoặc file có virus đi qua nó.

- Các cơ chế thiết lập firewall:

**+** Tất cả truy cập lưu lượng đến hoặc đi, internet đều phải đi qua firewall

**+** Chỉ lưu lượng được ủy quyền, như được xác định bởi chính sách bảo mật cục bộ mới có thể đi qua firewall.

**+** Bản thân firewall không bị xâm nhập. Nó là một hệ thống đáng tin cậy.

## 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

Cách thiết lập một bộ khóa trong thuật toán RSA:

1. Chọn 2 số nguyên tố lớn khác nhau p, q thỏa mãn điều kiện (lựa chọn ngẫu nhiên và độc lập)

2. Tính tích của p, q: n = p\*q;

3. Tính giá trị hàm số Euler của n: .

4. Tính1 số tự nhiên e sao cho 1<e< và là số nguyên tố cùng nhau với .

5. Chọn số nguyên d, sao cho và gcd (d, e) ≡ 1 (mod )

6. Khóa công khai bao gồm: n và e. Khóa bí mật gồm: n và d.

- Ứng dụng:

1) Chọn p = 11 và q = 3, do đó N = p\*q = 33 ( = 32 < 33 < 64 = )

2) n = (p-1) (q-1) = 20

3) Chọn e = 3 nguyên tố cùng nhau với n

4) Tính nghịch đảo của e trong phép modulo n được d = 7 (3x7 = 21)

5) Khóa công khai KU = (e, N) = (3, 33). Khóa bí mật KR = (d, N) = (7, 33)

6) Mã hóa bản rõ M = 15: C = mod N = 153 mod 33 = 9

7) Giải mã bản mã C = 9: M = mod N = 97 mod 33 = 15

## 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?

\* Hiểu biết về hàm băm:

- Một hàm băm thực hiện trên 1 thông điệp để tạo ra 1 giá trị băm.

- Thông điệp được băm được thay đổi nhỏ thì sẽ đưa ra 1 giá trị băm mới khác hoàn toàn nhau.

- Hàm băm thì băm trên các thông điệp khác nhau thì rất khó tạo ra giá trị băm giống nhau.

- Rất khó từ giá trị băm để suy ra được thông điệp gốc.

\* Sử dụng hàm băm trong đảm bảo tính toàn vẹn

- A gửi thông điệp M cho B thì A sẽ băm M để được 1 giá trị băm sau đó gán cùng với thông điệp M gửi cho B

- Bên B nhận được thông điệp lấy ra được thông điệp M sau đó băm M và so sánh 2 giá trị băm, nếu trùng khớp thì dữ liệu được toàn vẹn.

## 18. Nêu kiến trúc các mô hình cài đặt firewall?

**- Thứ nhất: Kiến trúc Dual-homed Host**

Được xây dựng dựa trên máy tính dual-home host. Một máy tính được gọi là dual-homed host nếu có ít nhất 2 network interface, có nghĩa là máy đó có gắn 2 card giao tiếp với 2 mạng khác nhau , do đó máy tính này đóng vai trò là router mềm, Kiến trúc dual-home host rất đơn giản, máy dual-home host ở giữa, một bên được nối với internet và bên còn lại nối với mạng nội bộ. Kiến trúc này có các đặc điểm sau:

+ Phải disable chức năng routing của dual-homed host để cấm hoàn toàn thông IP từ ngoài vào

+ Các hệ thống bên ngoài và bên trong dual-home host không liên lạc trực tiếp được với nhau.

+ Dual homed host cung cấp dịch vụ thông qua poxy server hoặc login trực tiếp vào dual –home host.

- **Thứ hai: Kiến trúc Screened Host**

Trong kiến trúc này chức năng bảo mật chính được cung cấp bởi chức năng packet filtering tại screening router. Packet filtering trên screening router được setup sao cho basition host là máy duy nhất trong internal network mà các host trên internet có thể mở kết nối đến Packet filtering cũng cho phép bastion host mở các kết nối ra bên ngoài. Các packet filtering thực hiện công việc sau:

+ Cho phép các interal hosts mở kết nối đến các host trên internet đối với một số dịch vụ được phép

+ Cấm tất cả kết nối từ các interal hosts

- **Thứ ba: Kiến trúc Screened Subnet Host**

Thêm một perimeter network để cô lập interal network với internet.Như vật dù hacker đã tấn công được vào bastion host vẫn còn một rào chắn nữa phải vượt qua interior router. Các lưu thông trong internet network được bảo vệ an toàn cho dù bastion đã bị “ chiếm”. Các dịch vụ nào ít tin cậy và có khả năng dễ bị tấn công thì nên để ở perimeter network.Bastion host là điệm liên lạc cho các kết nối từ ngoài vào :SMTP, FTP,DNS . Còn đối với viêc truy cập các dịch vụ từ internal client đến các server trên internet thì được điều khiển như sau:

Setup packet filtering trên các exterior và interior router để cho phép internal client truy cập các servers bên ngoài 1 cách trực tiếp.

Setup poxy server tren bastion host để cho phép internal clients truy cập các server bên ngoài 1 cách gián tiếp.

## 19. Trình bày về SQL Injection? Nêu ví dụ và cách khắc phục

**- SQL Injection** là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng. Được thực hiện bằng cách chèn thêm một đoạn SQL để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database. **SQL injection** có thể cho phép những kẻ tấn công thực hiện các thao tác như một người quản trị web, trên cơ sở dữ liệu của ứng dụng.

**- Cách khắc phục:**

+ Cách 1: Vô hiệu hóa các ký tự đặc biệt: loại bỏ các ký tự đặc biệt như dấu ngoặc kép, dấu nháy bằng đặt trước chúng dấu gạch chéo ngược. Hoặc sử dụng phương thức get\_magic\_quotes\_gpc() hoặc sử dụng phương thức real\_escape\_string() khi gọi đến MySQL.

+ Cách 2: Tham số hóa cho câu truy vấn: Không cho phép dữ liệu do người dùng gửi được hiểu là các câu lệnh MySQL. Câu lệnh truy vấn có thể sử dụng tham số ‘?’ như 1 từ thay thế cho dữ liệu.

## 20. Trình bày về Cross-Site Scripting (XSS)? Nêu ví dụ và cách khắc phục

* Cross Site Scripting có thể xảy ra trên tập lệnh độc hại được thực hiện ở phía client.
* Trang web hoặc form giả mạo được hiển thị cho người dùng (nơi nạn nhân nhập thông tin đăng nhập hoặc nhấp vào liên kết độc hại).
* Trên các trang web có quảng cáo được hiển thị.
* Email độc hại được gửi đến nạn nhân. Tấn công xảy ra khi tin tặc tìm kiếm những lỗ hổng trên website và gửi nó làm đầu vào độc hại. Tập lệnh độc hại được tiêm vào mã lệnh và sau đó được gửi dưới dạng đầu ra cho người dùng cuối cùng.

**Ví dụ:**

\*\*<script type=”text/javascript”>

Var test=’../example.php?cookie\_data=’+escape(docuent.cookie);

</script>\*\*

Như đã thấy trong Ví dụ trên, cookie bị mất và được gửi tới biến ‘cookie\_data’ của tập lệnh mẫu example.php. Nếu hacker sẽ chèn tập lệnh này vào mã của trang web, thì mã sẽ được thực thi trong trình duyệt của người dùng và cookie sẽ được gửi tới hacker.

**Cách khắc phục:**

Để ngăn chặn các cuộc tấn công XSS, điều quan trọng là phải triển khai các biện pháp bảo mật như xác thực đầu vào, mã hóa đầu ra, chính sách bảo mật nội dung(CSP), sử dụng HTTPS và sử dụng các biện pháp mã hóa an toàn. Ngoài ra, các nhà phát triển web nên biết về các loại tấn công XSS khác nhau, bao gồm XSS được phản ánh và XSS được lưu trữ, đồng thời thực hiện các biện pháp thích hợp để giảm thiểu những rủi ro này.

## 21. Trình bày về XML Injection? Nêu ví dụ và cách khắc phục

* Ngôn ngữ đánh dấu là một phương pháp thêm chú thích vào văn bản để phần bổ sung có thể được phân biệt với chính văn bản.
* XML là ngôn ngữ đánh dấu.
* XML được thiết kế để mang dữ liệu thay vì chỉ ra cách hiển thị nó.
* XML không có bộ thẻ được xác định trước; thay vào đó, người dùng xác định thẻ riêng của họ

**Ví dụ:**

<?xml version="1.0" encoding="UTF-8"?>

<application>

<title>eMB</title>

<company>MB</company>

<year>2021</year>

<price>40000000</price>

</application>

**Cách khắc phục:**

Để ngăn chặn các cuộc tấn công chèn XML, điều quan trọng là phải áp dụng các kỹ thuật giảm nhẹ tương tự như các kỹ thuật được sử dụng để chèn SQL:

* Xác thực và vệ sinh đầu vào của người dùng.
* Sử dụng các truy vấn XPath được tham số hóa hoặc các câu lệnh đã chuẩn bị sẵn.
* Sử dụng mã hóa đầu vào và mã hóa đầu ra thích hợp.
* Triển khai Chính sách bảo mật nội dung (CSP) để kiểm soát các nguồn tập lệnh.
* Thường xuyên cập nhật và vá lỗi phần mềm để khắc phục các lỗ hổng bảo mật.

Bằng cách áp dụng những phương pháp này, các nhà phát triển có thể giảm đáng kể nguy cơ bị tấn công chèn XML.

## 22. Trình bày về Directory Traversal/Command Injection? Nêu ví dụ về lỗi file upload và cách khắc phục

* Việc truyền tải thư mục sử dụng dữ liệu đầu vào không đúng định dạng hoặc lợi dụng một lỗ hổng di chuyển từ thư mục gốc tới các thư mục bị hạn chế.
* Khi kẻ tấn công đã truy cập vào một thư mục bị hạn chế, nó có thể truy cập (tiêm) các lệnh để thực thi trên máy chủ (được gọi là tiêm lệnh) hoặc xem các tập tin bí mật.

**Ví dụ:**

<?php

if ($\_SERVER['REQUEST\_METHOD'] === 'POST') {

$filename = $\_FILES["file"]["name"];

$target\_path = "uploads/" . $filename;

// Lưu hình ảnh vào thư mục uploads

move\_uploaded\_file($\_FILES["file"]["tmp\_name"], $target\_path);

// Hiển thị hình ảnh

echo "<img src='uploads/" . $filename . "' alt='Uploaded Image'>";

}

?>

Nếu người tấn công gửi một tệp tin với tên ../../../config.php, có thể truy cập vào tệp tin cấu hình và tiềm ẩn thông tin quan trọng

**Cách khắc phục:**

* Trước khi lưu hoặc sử dụng đường dẫn từ người dùng, kiểm tra và đảm bảo rằng nó chỉ trỏ đến thư mục cần thiết và không chứa các thành phần đường dẫn không mong muốn.
* Xử lý lỗi một cách an toàn để ngăn chặn người tấn công từ việc thu thập thông tin về cấu trúc hệ thống hoặc thực hiện các tấn công Directory Traversal.
* Lưu trữ tệp tin tải lên ngoài thư mục web root để ngăn chặn việc thực thi trực tiếp của tệp tin thông qua trình duyệt.
* Sử dụng hàm hash (ví dụ: MD5) cho tên tệp tin để tránh việc sử dụng các tên tệp tin có thể được kiểm soát bởi người tấn công.

## 23. Trình bày một số hình thức tấn công phía client: Header manipulation, Cookies

## Header manipulation:

* Tiêu đề HTTP bao gồm các trường chứa thông tin về đặc điểm của dữ liệu được truyền
* Kẻ tấn công có thể sửa đổi các tiêu đề HTTP để tạo ra một cuộc tấn công bằng cách sử dụng thao tác tiêu đề HTTP.
* Thao tác tiêu đề HTTP không phải là một cuộc tấn công thực sự mà là phương tiện mà qua đó các cuộc tấn công khác, chẳng hạn như XSS, có thể được thực hiện

**Cookies:**

* Cookie có thể chứa nhiều thông tin khác nhau dựa trên thông tin của người dùng sở thích khi truy cập một trang web.
* Tồn tại một số loại cookie khác nhau: Cookie của bên thứ nhất, Bên thứ ba cookie, cookie phiên.
* Cookie của bên thứ nhất có thể bị đánh cắp và sử dụng để mạo danh người dùng.
* Cookie của bên thứ ba có thể được sử dụng để theo dõi việc duyệt hoặc mua thói quen của người sử dụng.

## 24. Trình bày hình thức tấn công phía client: Attachments, Session Hijacking

## Attachments:

* Tệp đính kèm là các tệp được ghép nối với thư email.
* Các tệp đính kèm độc hại thường được sử dụng để phát tán vi-rút, Trojan, và phần mềm độc hại khác khi chúng được mở

**Session Hijacking:**

Chiếm quyền điều khiển phiên là một cuộc tấn công trong đó kẻ tấn công cố gắng mạo danh người dùng bằng cách sử dụng mã thông báo phiên của nó.

## 25. Trình bày về DoS và các loại tấn công DoS

* Tấn công DoS là một nỗ lực có chủ ý nhằm ngăn chặn người dùng được ủy quyền truy cập vào một hệ thống bằng cách áp đảo hệ thống đó bằng các yêu cầu.
* Hầu hết các cuộc tấn công DoS ngày nay thực chất là từ chối dịch vụ phân tán (DDoS): thay vì sử dụng một máy tính, DDoS có thể sử dụng hàng trăm hoặc hàng nghìn máy tính zombie trong một mạng botnet để tấn công thiết bị có yêu cầu.

**Các loại tấn công:**

**Ping flood**

Nhiều máy tính nhanh chóng gửi một lượng lớn tiếng vang ICMP yêu cầu, áp đảo máy chủ (cũng như mạng) tới đến mức nó không thể đáp ứng đủ nhanh và sẽ loại bỏ các kết nối với các máy khách khác và từ chối mọi kết nối mới.

**Smurf attack**

* Kẻ tấn công phát tán yêu cầu ping tới tất cả các máy tính trên mạng nhưng thay đổi địa chỉ mà từ đó yêu cầu đến máy tính của nạn nhân.
* Sau đó, mỗi máy tính sẽ gửi phản hồi tới địa chỉ của nạn nhân. khiến máy tính nhanh chóng bị quá tải và sau đó bị treo hoặc trở nên không có sẵn cho người dùng hợp pháp.

**SYN flood**

SYN flood (half-open attack) là một kiểu tấn công từ chối dịch vụ (DDos). Tấn công này với mục đích làm cho Server không có lưu lượng để truy cập hợp pháp. Bằng cách tiêu thụ tất cả tài nguyên server đang có sẵn. Người tấn công có thể áp đảo tất cả các cổng trên Server. Làm cho thiết bị Client đáp ứng lưu lượng hợp pháp một cách chậm chạp.

## 26. Trình bày về Interception, Poisioning và các hình thức tấn công chiếm quyền truy cập (Access Rights)

**Interception**

* Cuộc tấn công lặp lại tương tự như cuộc tấn công trung gian thụ động.
* Kẻ tấn công tạo một bản sao của đường truyền trước khi gửi nó đến người nhận. Sau đó, kẻ tấn công có thể gửi tin nhắn gốc tới máy chủ và máy chủ có thể phản hồi. Bây giờ một mối quan hệ đáng tin cậy đã được thiết lập giữa kẻ tấn công và máy chủ.
* Kẻ tấn công có thể bắt đầu thay đổi nội dung của ảnh bị bắt tin nhắn và mã. Nếu cuối cùng anh ấy thực hiện sửa đổi chính xác, máy chủ sẽ phản hồi, cho kẻ tấn công biết anh ta đã thành công

**Poisioning**

* ARP Poisoning: Kẻ tấn công có thể sửa đổi địa chỉ MAC trong ARP cache để địa chỉ IP tương ứng trỏ tới một địa chỉ khác máy tính
* DNS Poisoning là quá trình thay thế một địa chỉ DNS để máy tính được tự động chuyển hướng sang thiết bị khác

**Access Rights**

* Nâng cao đặc quyền: đang khai thác lỗ hổng trong phần mềm để đạt được quyền truy cập vào các tài nguyên mà người dùng thường bị hạn chế truy cập.
* Truy cập bắc cầu: Hệ thống A có thể truy cập Hệ thống B và vì Hệ thống B có thể truy cập Hệ thống C, sau đó Hệ thống A có thể truy cập Hệ thống C.