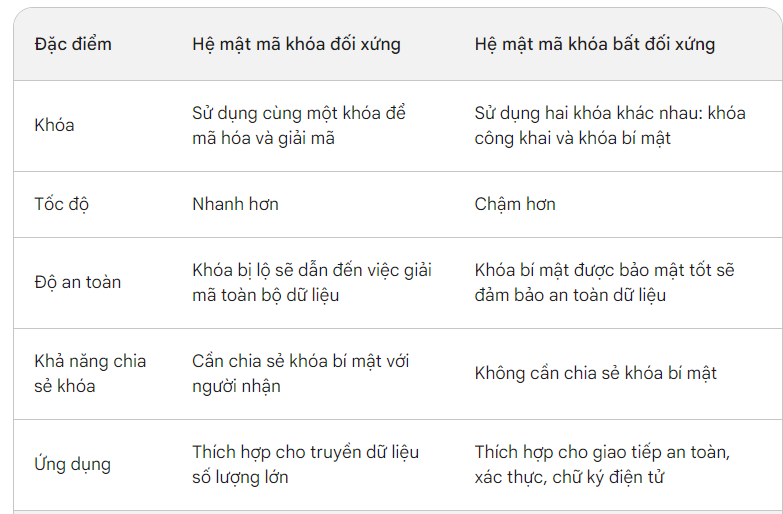
**Câu 1. Anh/chị hãy so sánh đặc điểm của hệ mật mã khóa đối xứng với hệ mật mã khóa bất đối xứng?**



**Câu 2. Anh/chị hãy giải thích tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống thông tin?**

**1. Bảo vệ tài sản:**

* Thông tin và hệ thống thông tin là tài sản quan trọng của cá nhân, tổ chức, doanh nghiệp.
* Việc đảm bảo an toàn giúp bảo vệ tài sản khỏi các mối đe dọa như đánh cắp, phá hủy, sửa đổi trái phép.

**2. Đảm bảo tính bí mật:**

* Nhiều thông tin có tính chất bí mật, cần được bảo vệ khỏi những người truy cập trái phép.
* Việc đảm bảo an toàn giúp bảo vệ tính bí mật của thông tin cá nhân, thông tin kinh doanh, bí mật nhà nước, v.v.

**3. Duy trì tính toàn vẹn:**

* Thông tin và hệ thống thông tin cần được bảo vệ khỏi các hành vi sửa đổi trái phép.
* Việc đảm bảo an toàn giúp duy trì tính toàn vẹn, chính xác và đáng tin cậy của thông tin.

**4. Đảm bảo tính sẵn sàng:**

* Hệ thống thông tin cần hoạt động liên tục để phục vụ nhu cầu của người dùng.
* Việc đảm bảo an toàn giúp hệ thống thông tin hoạt động ổn định, tránh các sự cố gián đoạn hoặc ngừng hoạt động.

**5. Giảm thiểu rủi ro:**

* Các mối đe dọa an ninh mạng có thể gây ra nhiều rủi ro cho cá nhân, tổ chức, doanh nghiệp.
* Việc đảm bảo an toàn giúp giảm thiểu rủi ro tài chính, rủi ro pháp lý, rủi ro danh tiếng, v.v.

**6. Nâng cao hiệu quả hoạt động:**

* Hệ thống thông tin an toàn giúp nâng cao hiệu quả hoạt động, tăng năng suất và khả năng cạnh tranh.
* Việc đảm bảo an toàn giúp tiết kiệm chi phí và thời gian cho việc khắc phục các sự cố an ninh mạng.

**7. Tuân thủ quy định pháp luật:**

* Nhiều quốc gia có luật pháp về an ninh mạng yêu cầu các tổ chức phải bảo vệ thông tin và hệ thống thông tin.
* Việc đảm bảo an toàn giúp tuân thủ các quy định pháp luật và tránh các hình phạt.

**8. Tăng cường niềm tin:**

* Khách hàng, đối tác và nhà đầu tư sẽ tin tưởng hơn vào các tổ chức có hệ thống thông tin an toàn.
* Việc đảm bảo an toàn giúp tăng cường niềm tin và tạo dựng uy tín cho tổ chức.

**Câu 3. Anh/chị hãy giải thích các lớp phòng vệ điển hình trong mô hình đảm bảo an toàn hệ thống thông tin có chiều sâu Defence in Depth?**

Mô hình Defence in Depth (D in D) là một chiến lược an ninh mạng tập trung vào việc xây dựng nhiều lớp phòng vệ để bảo vệ hệ thống thông tin. Mỗi lớp phòng vệ đóng vai trò như một rào cản, giúp ngăn chặn hoặc làm chậm kẻ tấn công xâm nhập vào hệ thống.

Dưới đây là các lớp phòng vệ điển hình trong mô hình D in D:

**1. Vành đai an ninh (Perimeter security):**

Lớp này bao gồm các biện pháp bảo vệ bên ngoài hệ thống, như tường lửa, hệ thống phát hiện xâm nhập (IDS), hệ thống ngăn chặn xâm nhập (IPS), mạng riêng ảo (VPN), v.v. Lớp này giúp ngăn chặn các truy cập trái phép từ bên ngoài vào hệ thống.

**2. An ninh mạng (Network security):**

Lớp này bao gồm các biện pháp bảo vệ mạng nội bộ, như phân chia mạng, kiểm soát truy cập mạng, mã hóa dữ liệu truyền tải, v.v. Lớp này giúp bảo vệ dữ liệu và hệ thống nội bộ khỏi các truy cập trái phép từ bên trong mạng.

**3. An ninh điểm cuối (Endpoint security):**

Lớp này bao gồm các biện pháp bảo vệ các thiết bị đầu cuối như máy tính, điện thoại thông minh, máy tính bảng, v.v. Lớp này giúp bảo vệ dữ liệu và hệ thống trên các thiết bị đầu cuối khỏi các phần mềm độc hại, tấn công zero-day, v.v.

**4. An ninh ứng dụng (Application security):**

Lớp này bao gồm các biện pháp bảo vệ các ứng dụng phần mềm, như kiểm tra mã nguồn, kiểm tra bảo mật ứng dụng, mã hóa dữ liệu ứng dụng, v.v. Lớp này giúp bảo vệ ứng dụng khỏi các lỗ hổng bảo mật và các cuộc tấn công nhắm vào ứng dụng.

**5. An ninh dữ liệu (Data security):**

Lớp này bao gồm các biện pháp bảo vệ dữ liệu, như sao lưu dữ liệu, mã hóa dữ liệu, kiểm soát truy cập dữ liệu, v.v. Lớp này giúp bảo vệ dữ liệu khỏi các truy cập trái phép, mất mát hoặc hư hỏng.

**6. An ninh vật lý (Physical security):**

Lớp này bao gồm các biện pháp bảo vệ hệ thống thông tin khỏi các mối đe dọa vật lý, như kiểm soát ra vào, giám sát camera, bảo vệ chống cháy nổ, v.v. Lớp này giúp bảo vệ hệ thống thông tin khỏi các hành vi phá hoại, trộm cắp hoặc truy cập trái phép vào cơ sở hạ tầng vật lý.

**7. Giáo dục và nhận thức (Education and awareness):**

Lớp này bao gồm việc nâng cao nhận thức của người dùng về an ninh mạng và các biện pháp phòng ngừa. Lớp này giúp giảm thiểu rủi ro do lỗi của người dùng, như sử dụng mật khẩu yếu hoặc mở email độc hại.

**Câu 4. Anh/chị hãy giải thích các thuộc tính an ninh an toàn của hệ thống thông tin theo mô hình CIA?**

**Các thuộc tính an ninh an toàn của hệ thống thông tin theo mô hình CIA:**

Mô hình CIA là một mô hình bảo mật thông tin phổ biến được sử dụng để đánh giá mức độ an toàn của hệ thống thông tin. Mô hình CIA bao gồm 3 thuộc tính chính:

**1. Bí mật (Confidentiality):**

* **Định nghĩa:** Đảm bảo rằng thông tin chỉ được truy cập bởi những người được phép.
* **Ví dụ:** Sử dụng mật khẩu, mã hóa dữ liệu, kiểm soát truy cập.
* **Mục tiêu:** Bảo vệ thông tin nhạy cảm khỏi bị tiết lộ trái phép.

**2. Toàn vẹn (Integrity):**

* **Định nghĩa:** Đảm bảo rằng thông tin là chính xác, đầy đủ và không bị thay đổi trái phép.
* **Ví dụ:** Sử dụng checksum, kiểm tra tính hợp lệ dữ liệu, sao lưu dữ liệu.
* **Mục tiêu:** Bảo vệ tính chính xác và độ tin cậy của thông tin.

**3. Sẵn sàng (Availability):**

* **Định nghĩa:** Đảm bảo rằng thông tin luôn sẵn sàng cho những người được phép truy cập.
* **Ví dụ:** Sử dụng các biện pháp dự phòng, cân bằng tải, giám sát hệ thống.
* **Mục tiêu:** Đảm bảo người dùng có thể truy cập thông tin khi cần thiết.

**Câu 5. Anh/chị hãy giải thích quan hệ giữa mối đe dọa và lỗ hổng trong hệ thống thông tin và liệt kê các mối đe dọa thường gặp?**

**Mối đe dọa** là một sự kiện hoặc hành động có khả năng gây hại cho hệ thống thông tin. **Lỗ hổng** là một điểm yếu trong hệ thống thông tin có thể bị kẻ tấn công lợi dụng để thực hiện hành vi xâm nhập hoặc phá hoại.

**Mối quan hệ giữa mối đe dọa và lỗ hổng:**

* Mối đe dọa cần có lỗ hổng để có thể khai thác và gây hại cho hệ thống thông tin.
* Một lỗ hổng có thể bị nhiều mối đe dọa khác nhau khai thác.
* Mức độ rủi ro của một hệ thống thông tin phụ thuộc vào cả mức độ nghiêm trọng của mối đe dọa và mức độ nghiêm trọng của lỗ hổng.

**Câu 6. Anh/chị hãy giải thích quan hệ giữa mối đe dọa và lỗ hổng trong hệ thống thông tin và liệt kê các mối đe dọa thường gặp?**

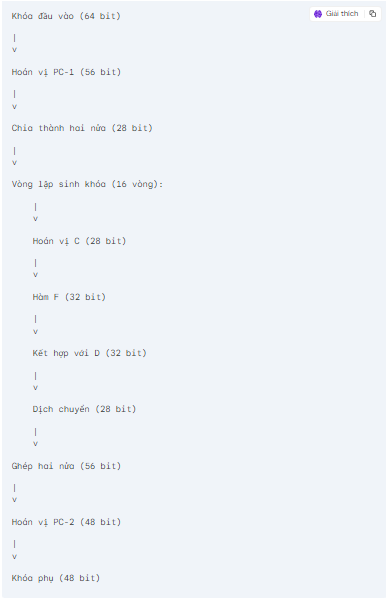
**Mối đe dọa** là một sự kiện hoặc hành động có khả năng gây hại cho hệ thống thông tin. **Lỗ hổng** là một điểm yếu trong hệ thống thông tin có thể bị kẻ tấn công lợi dụng để thực hiện hành vi xâm nhập hoặc phá hoại.

**Mối quan hệ giữa mối đe dọa và lỗ hổng:**

* **Mối đe dọa cần có lỗ hổng để có thể khai thác và gây hại cho hệ thống thông tin.** Ví dụ, virus máy tính cần có lỗ hổng bảo mật trong phần mềm để có thể lây nhiễm vào hệ thống.
* **Một lỗ hổng có thể bị nhiều mối đe dọa khác nhau khai thác.** Ví dụ, một lỗ hổng trong hệ thống web có thể bị khai thác để thực hiện tấn công SQL injection hoặc cross-site scripting.
* **Mức độ rủi ro của một hệ thống thông tin phụ thuộc vào cả mức độ nghiêm trọng của mối đe dọa và mức độ nghiêm trọng của lỗ hổng.** Ví dụ,

**Câu 7. Anh/chị hãy vẽ sơ đồ cấp và sử dụng chứng chỉ số, giải thích sơ đồ?**

**Câu 8. Trong hệ mã hóa DES, anh/chị hãy vẽ sơ đồ thuật toán các bước sinh khóa phụ của hệ mã, giải thích sơ đồ?**



**Câu 9. Anh/chị hãy so sánh 2 loại phần mềm độc hại: virus và worm?**

**Điểm giống nhau:**

* **Cả hai đều là phần mềm độc hại:** Virus và worm đều có khả năng lây lan từ máy tính này sang máy tính khác và gây hại cho hệ thống.
* **Khả năng lây lan:** Virus và worm đều có khả năng tự sao chép và lây lan sang các máy tính khác.
* **Gây hại cho hệ thống:** Virus và worm đều có khả năng gây hại cho hệ thống như: đánh cắp dữ liệu, phá hủy hệ thống, làm gián đoạn hoạt động của hệ thống.

**Điểm khác nhau:**



**Câu 10. Anh/chị hãy trình bày về biện pháp điều khiển truy nhập DAC và cho ví dụ?**

**Định nghĩa:**

**Điều khiển truy cập tùy quyền (DAC)** là một mô hình kiểm soát truy cập dựa trên nguyên tắc chủ sở hữu của dữ liệu. Theo mô hình DAC, chủ sở hữu của dữ liệu có quyền quyết định ai có thể truy cập dữ liệu của họ và với quyền gì.

**Đặc điểm:**

* **Dựa trên chủ sở hữu:** Chủ sở hữu dữ liệu có quyền kiểm soát truy cập.
* **Tính linh hoạt:** Chủ sở hữu có thể cấp quyền truy cập cho bất kỳ ai họ muốn.
* **Đơn giản:** Dễ dàng triển khai và quản lý.

**Cách thức hoạt động:**

* **Chủ sở hữu** của dữ liệu tạo ra một **danh sách kiểm soát truy cập (ACL)**.
* ACL liệt kê các **tài khoản người dùng** và **quyền truy cập** của họ đối với dữ liệu.
* Khi một **người dùng** yêu cầu truy cập dữ liệu, hệ thống sẽ kiểm tra ACL để xác định xem người dùng đó có được phép truy cập hay không.

**Ví dụ:**

* **Hệ thống tập tin:** Trong hệ thống tập tin, chủ sở hữu của một tập tin có thể cấp quyền truy cập cho người dùng khác để đọc, ghi hoặc sửa đổi tập tin.
* **Email:** Người dùng có thể đặt quyền truy cập cho phép người khác đọc, gửi hoặc xóa email của họ.
* **Mạng xã hội:** Người dùng có thể đặt quyền truy cập cho phép người khác xem trang cá nhân của họ, bài đăng của họ hoặc ảnh của họ.

**Câu 11. Anh/chị hãy phân tích các kỹ thuật kiểm soát truy nhập trên tường lửa? Liệt kê các hạn chế của tường lửa?**

## Kỹ thuật kiểm soát truy nhập trên tường lửa:

Tường lửa sử dụng các kỹ thuật sau để kiểm soát truy cập:

**1. Lọc gói tin:**

* Tường lửa phân tích các gói tin IP dựa trên các quy tắc được định nghĩa trước.
* Các quy tắc này xác định các gói tin nào được phép đi qua tường lửa và các gói tin nào bị chặn.
* Lọc gói tin có thể dựa trên các yếu tố như địa chỉ IP nguồn và đích, cổng TCP/UDP, giao thức, v.v.

**2. Danh sách kiểm soát truy cập (ACL):**

* ACL là một tập hợp các quy tắc xác định các quyền truy cập được phép cho các tài nguyên mạng.
* ACL có thể được áp dụng cho các cổng, địa chỉ IP, giao thức, v.v.
* ACL có thể cho phép hoặc cấm truy cập dựa trên các tiêu chí cụ thể.

**3. Dịch địa chỉ mạng (NAT):**

* NAT che giấu địa chỉ IP thực của các máy tính trong mạng nội bộ khỏi mạng bên ngoài.
* NAT giúp bảo vệ mạng nội bộ khỏi các tấn công mạng.
* NAT cũng có thể được sử dụng để kiểm soát truy cập bằng cách chỉ cho phép các kết nối từ các địa chỉ IP được phép.

**4. Vùng an ninh:**

* Tường lửa có thể chia mạng thành các vùng an ninh với các mức độ bảo mật khác nhau.
* Các vùng an ninh có thể được phân biệt dựa trên chức năng, mức độ tin cậy hoặc mức độ nhạy cảm của dữ liệu.
* Việc sử dụng các vùng an ninh giúp hạn chế truy cập trái phép vào các khu vực nhạy cảm của mạng.

**5. Xác thực:**

* Tường lửa có thể yêu cầu người dùng xác thực trước khi truy cập vào mạng nội bộ.
* Xác thực có thể được thực hiện bằng cách sử dụng mật khẩu, token, chứng chỉ, v.v.
* Việc sử dụng xác thực giúp tăng cường bảo mật mạng và ngăn chặn truy cập trái phép.

## Hạn chế của tường lửa:

* **Tường lửa không thể bảo vệ khỏi tất cả các mối đe dọa:** Tường lửa chỉ có thể bảo vệ khỏi các mối đe dọa được biết đến và được cấu hình để chặn.
* **Tường lửa có thể bị tấn công:** Tường lửa có thể bị tấn công bởi các hacker có kinh nghiệm.
* **Tường lửa có thể làm giảm hiệu suất mạng:** Việc kiểm tra và lọc các gói tin có thể làm giảm tốc độ mạng.
* **Tường lửa có thể khó cấu hình:** Việc cấu hình tường lửa có thể phức tạp và yêu cầu kiến thức chuyên môn.
* **Tường lửa không thể thay thế cho các biện pháp bảo mật khác:** Tường lửa chỉ là một phần của hệ thống bảo mật tổng thể.

**Câu 12. Anh/chị hãy vẽ sơ đồ quá trình tạo và kiểm tra chữ ký số, giải thích sơ đồ?**

**Câu 13. Anh/chị hãy giải thích tấn công kiểu Social Engineering và nêu các cách phòng chống?**

**Định nghĩa:**

Tấn công Social Engineering là kỹ thuật thao túng tâm lý con người để đánh cắp thông tin hoặc thực hiện hành vi trái phép. Kẻ tấn công sẽ lợi dụng lòng tin, sự sơ hở hoặc thiếu cảnh giác của người dùng để đạt được mục đích.

**Cách thức hoạt động:**

* **Thu thập thông tin:** Kẻ tấn công sẽ thu thập thông tin về mục tiêu, bao gồm tên, địa chỉ, số điện thoại, email, v.v.
* **Xây dựng mối quan hệ:** Kẻ tấn công sẽ xây dựng mối quan hệ với mục tiêu để tạo dựng lòng tin.
* **Thực hiện tấn công:** Kẻ tấn công sẽ sử dụng các kỹ thuật thao túng tâm lý để dụ dỗ mục tiêu tiết lộ thông tin nhạy cảm hoặc thực hiện hành vi trái phép.

**Ví dụ:**

* **Lừa đảo qua điện thoại:** Kẻ tấn công giả mạo nhân viên ngân hàng hoặc cơ quan chức năng để lừa người dùng tiết lộ thông tin tài khoản hoặc chuyển tiền.
* **Tấn công phishing:** Kẻ tấn công gửi email giả mạo hoặc tin nhắn giả mạo để dụ dỗ người dùng click vào liên kết độc hại hoặc tải xuống tập tin đính kèm chứa virus.
* **Tấn công baiting:** Kẻ tấn công đặt USB hoặc thiết bị lưu trữ khác chứa virus tại nơi công cộng để dụ dỗ người dùng cắm vào máy tính của họ.

**Cách phòng chống:**

* **Nâng cao nhận thức:** Nâng cao nhận thức về các loại tấn công Social Engineering và cách thức hoạt động của chúng.
* **Cẩn thận với thông tin cá nhân:** Không tiết lộ thông tin cá nhân cho người lạ hoặc qua các kênh không an toàn.
* **Xác minh thông tin:** Xác minh thông tin trước khi thực hiện bất kỳ hành động nào, chẳng hạn như chuyển tiền hoặc click vào liên kết.
* **Cài đặt phần mềm bảo mật:** Cài đặt phần mềm bảo mật để bảo vệ máy tính khỏi virus và phần mềm độc hại.
* **Cập nhật phần mềm:** Cập nhật phần mềm thường xuyên để vá các lỗ hổng bảo mật.

**Câu 14, Anh/chị hãy cho biết các thành phần và chức năng của hạ tầng quản lý khóa công khai PKI?**

## Các thành phần và chức năng của hạ tầng quản lý khóa công khai PKI:

**Thành phần:**

* **Trung tâm chứng thực (CA):** CA là thực thể chịu trách nhiệm cấp phát, quản lý và thu hồi các chứng chỉ số. CA đóng vai trò trung gian đáng tin cậy trong hệ thống PKI.
* **Chứng chỉ số:** Chứng chỉ số là một tập tin điện tử chứa thông tin về chủ sở hữu khóa công khai, được CA xác nhận và ký bằng chữ ký số của CA.
* **Khóa công khai và khóa bí mật:** Khóa công khai được sử dụng để mã hóa thông tin, trong khi khóa bí mật được sử dụng để giải mã thông tin.
* **Lưu trữ khóa:** Lưu trữ khóa là nơi lưu trữ an toàn các khóa bí mật của người dùng.
* **Cơ quan đăng ký (RA):** RA là thực thể chịu trách nhiệm xác thực danh tính của người dùng trước khi CA cấp phát chứng chỉ số cho họ.

**Chức năng:**

* **Cấp phát chứng chỉ số:** CA cấp phát chứng chỉ số cho người dùng sau khi xác thực danh tính của họ.
* **Quản lý chứng chỉ số:** CA quản lý vòng đời của các chứng chỉ số, bao gồm việc cấp phát, gia hạn, thu hồi và cập nhật.
* **Thu hồi chứng chỉ số:** CA thu hồi chứng chỉ số khi cần thiết, chẳng hạn như khi khóa bí mật bị lộ hoặc khi người dùng không còn sử dụng chứng chỉ.
* **Xác thực danh tính:** RA xác thực danh tính của người dùng trước khi CA cấp phát chứng chỉ số cho họ.
* **Lưu trữ khóa:** Lưu trữ khóa lưu trữ an toàn các khóa bí mật của người dùng.
* **Mã hóa và giải mã:** Khóa công khai được sử dụng để mã hóa thông tin, trong khi khóa bí mật được sử dụng để giải mã thông tin.

**Câu 15. Trong hệ mã hóa DES, anh/chị hãy vẽ sơ đồ thuật toán các bước xử lý chính của hệ mã, giải thích sơ đồ?**

**Câu 16. Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên chữ ký của hệ thống IDS/IPS?**

Hệ thống phát hiện xâm nhập dựa trên chữ ký (signature-based intrusion detection system/intrusion prevention system - IDS/IPS) hoạt động bằng cách so sánh lưu lượng mạng hoặc nhật ký dữ liệu với cơ sở dữ liệu gồm các mẫu tấn công đã biết. Cơ chế này tương tự như cách phần mềm diệt virus hoạt động.

**Cách thức hoạt động:**

1. **Thu thập dữ liệu:** Hệ thống IDS/IPS thu thập dữ liệu mạng hoặc nhật ký dữ liệu từ các thiết bị được giám sát.
2. **Phân tích dữ liệu:** Hệ thống IDS/IPS phân tích dữ liệu thu thập được để tìm kiếm các mẫu tấn công đã biết.
3. **So sánh với cơ sở dữ liệu chữ ký:** Hệ thống IDS/IPS so sánh dữ liệu phân tích được với cơ sở dữ liệu chữ ký gồm các mẫu tấn công đã biết.
4. **Báo động:** Nếu hệ thống IDS/IPS phát hiện ra mẫu tấn công phù hợp, nó sẽ báo động cho người quản trị hệ thống.

**Câu 17. Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên bất thường của hệ thống IDS/IPS?**

Hệ thống phát hiện xâm nhập dựa trên bất thường (anomaly-based intrusion detection system/intrusion prevention system - IDS/IPS) hoạt động bằng cách phân tích lưu lượng mạng hoặc nhật ký dữ liệu để tìm kiếm các hoạt động bất thường có thể là dấu hiệu của một cuộc tấn công.

**Cách thức hoạt động:**

1. **Thu thập dữ liệu:** Hệ thống IDS/IPS thu thập dữ liệu mạng hoặc nhật ký dữ liệu từ các thiết bị được giám sát.
2. **Phân tích dữ liệu:** Hệ thống IDS/IPS sử dụng các thuật toán thống kê hoặc học máy để phân tích dữ liệu thu thập được.
3. **Xác định bất thường:** Hệ thống IDS/IPS xác định các hoạt động bất thường có thể là dấu hiệu của một cuộc tấn công.
4. **Báo động:** Nếu hệ thống IDS/IPS phát hiện ra hoạt động bất thường, nó sẽ báo động cho người quản trị hệ thống.

**Câu 18. Anh/chị hãy giải thích tấn công giả mạo địa chỉ và nêu cách phòng chống?**

**Định nghĩa:**

Tấn công giả mạo địa chỉ là kỹ thuật mà kẻ tấn công giả mạo địa chỉ IP hoặc địa chỉ MAC của một thiết bị khác để thực hiện các hành vi độc hại.

**Cách thức hoạt động:**

* **Giả mạo IP (IP Spoofing):** Kẻ tấn công gửi các gói tin với địa chỉ IP nguồn giả mạo để che giấu danh tính của họ hoặc để lừa dối các thiết bị khác thực hiện các hành động không mong muốn.
* **Giả mạo MAC (MAC Spoofing):** Kẻ tấn công thay đổi địa chỉ MAC của thiết bị mạng để truy cập trái phép vào mạng hoặc để đánh cắp dữ liệu.

**Mục đích:**

* **Tấn công từ chối dịch vụ (DoS):** Kẻ tấn công có thể sử dụng tấn công giả mạo địa chỉ để gửi lượng lớn lưu lượng truy cập giả mạo đến một máy chủ hoặc dịch vụ, khiến cho máy chủ hoặc dịch vụ đó bị quá tải và không thể truy cập được.
* **Lừa đảo:** Kẻ tấn công có thể sử dụng tấn công giả mạo địa chỉ để giả mạo là một người dùng hoặc thiết bị khác để lừa người dùng tiết lộ thông tin nhạy cảm hoặc thực hiện các hành động không mong muốn.
* **Truy cập trái phép:** Kẻ tấn công có thể sử dụng tấn công giả mạo địa chỉ để truy cập trái phép vào mạng hoặc thiết bị khác.

**Cách phòng chống:**

* **Sử dụng tường lửa:** Tường lửa có thể được cấu hình để chặn các gói tin có địa chỉ IP nguồn hoặc địa chỉ MAC giả mạo.
* **Sử dụng mạng riêng ảo (VPN):** VPN mã hóa lưu lượng truy cập mạng của bạn, giúp bảo vệ bạn khỏi các cuộc tấn công giả mạo địa chỉ.
* **Cập nhật phần mềm:** Cập nhật phần mềm thường xuyên để vá các lỗ hổng bảo mật có thể bị kẻ tấn công khai thác để thực hiện tấn công giả mạo địa chỉ.
* **Nâng cao nhận thức:** Nâng cao nhận thức về các mối đe dọa tấn công giả mạo địa chỉ và cách thức bảo vệ bản thân khỏi các cuộc tấn công này.

**Câu 19. Anh/chị hãy trình bày về cơ chế điều khiển truy nhập MAC và cho ví dụ?**

**Định nghĩa:**

Cơ chế điều khiển truy nhập MAC (Media Access Control) là phương pháp sử dụng địa chỉ MAC (địa chỉ vật lý) của thiết bị để kiểm soát quyền truy cập vào mạng hoặc tài nguyên mạng.

**Cách thức hoạt động:**

1. **Thiết lập danh sách kiểm soát truy cập (ACL):** ACL là danh sách các địa chỉ MAC được phép truy cập vào mạng hoặc tài nguyên mạng.
2. **Kiểm tra địa chỉ MAC:** Khi thiết bị cố gắng truy cập mạng hoặc tài nguyên mạng, thiết bị chuyển mạch hoặc bộ định tuyến sẽ kiểm tra địa chỉ MAC của thiết bị đó với ACL.
3. **Cho phép hoặc từ chối truy cập:** Nếu địa chỉ MAC của thiết bị nằm trong ACL, thiết bị được phép truy cập mạng hoặc tài nguyên mạng. Nếu địa chỉ MAC của thiết bị không nằm trong ACL,

**Câu 20. Anh/chị hãy trình bày sơ đồ phân loại và cách phòng chống các phần mềm độc hại**

## Sơ đồ phân loại phần mềm độc hại:

**1. Theo mục đích:**

* **Virus:** Lây nhiễm và phá hủy hệ thống.
* **Worm:** Tự sao chép và lây lan qua mạng.
* **Trojan:** Giả mạo phần mềm hợp pháp để đánh lừa người dùng.
* **Backdoor:** Cung cấp quyền truy cập trái phép cho kẻ tấn công.
* **Spyware:** Theo dõi và thu thập thông tin của người dùng.
* **Ransomware:** Mã hóa dữ liệu và đòi tiền chuộc.

**2. Theo phương thức lây nhiễm:**

* **Virus tệp tin:** Lây nhiễm vào các tệp tin thực thi.
* **Virus macro:** Lây nhiễm vào các tệp tin macro của Microsoft Office.
* **Virus boot sector:** Lây nhiễm vào sector khởi động của ổ đĩa.
* **Worm mạng:** Lây lan qua mạng bằng cách khai thác các lỗ hổng bảo mật.

## Cách phòng chống phần mềm độc hại:

**1. Phòng ngừa:**

* Cài đặt phần mềm diệt virus và cập nhật thường xuyên.
* Sử dụng tường lửa để bảo vệ máy tính khỏi các truy cập trái phép.
* Cẩn thận khi mở email và tệp đính kèm từ những người không quen biết.
* Không tải xuống phần mềm từ các nguồn không tin cậy.
* Cập nhật hệ điều hành và phần mềm thường xuyên để vá các lỗ hổng bảo mật.

**2. Phát hiện:**

* Sử dụng phần mềm diệt virus để quét virus thường xuyên.
* Theo dõi các hoạt động bất thường của hệ thống.
* Sử dụng các công cụ bảo mật khác như phần mềm chống phần mềm gián điệp và phần mềm chống lừa đảo.

**3. Xóa bỏ:**

* Sử dụng phần mềm diệt virus để xóa virus.
* Khôi phục hệ thống từ bản sao lưu nếu cần thiết.
* Thay đổi mật khẩu cho các tài khoản trực tuyến.