Câu 1: Anh/chi hãy giải thích tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống thông tin?

*-Do chúng ta đang sống trong thời đại công nghệ số, mọi thiết bị đều kết nối với Internet đó có nhiều nguy cơ, đe doạ mất an toàn thông tin, hệ thống thông tin:*

*+Có nguy cơ bị nghe trộm, đánh cắp và sửa đổi thông*

*+Bị tấn công từ tin tặc nhằm đánh cắp thông tin*

*+Lây nhiễm các phần mềm độc hại*

*+Lỗi hoặc các khuyết điểm phần cứng, phần mềm.*

Câu 2: 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 hệ thông thông tin theo mô hình CIA là việc đảm bảo ba thuộc tính của thông tin hoặc hệ thống bao gồm:  
+Tính bí mật (Confidentiality): Đảm bảo rằng chỉ người dùng có thẩm quyền mới được truy nhập thông tin hệ thống. (Thông tin cá nhân, thông tin bí mật quốc gia, quyền sở hữu trí tuệ).*

*+Tính toàn vẹn (Integrity): Đảm bảo thông tin và dữ liệu chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền.*

*+Tính sẵn dùng (Availability): Đảm bảo thông tin hoặc hệ thống có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu.*

Câu 3: Anh/chị hãy so sánh 2 loại phần mềm độc hại virus và worm ?

*-*

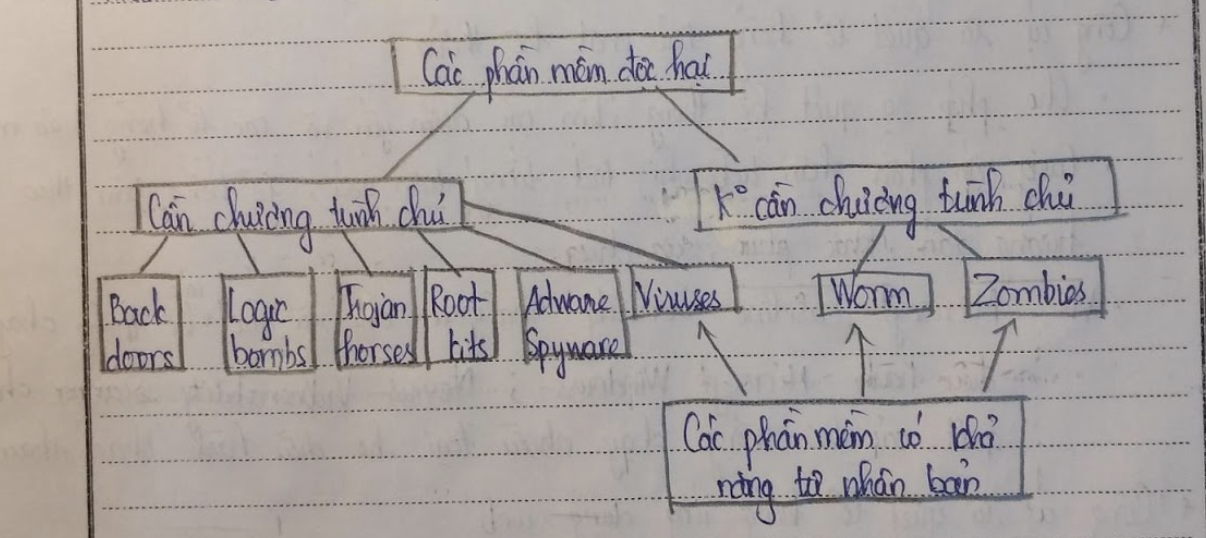
**

Câu 4: Anh/chị hãy trình bày sơ đồ phân loại và cách phòng chống các phần mềm đọc hại?

*-Các phần mềm độc hại chia thành 2 nhóm chính:*

*+Các phần mềm độc haiuj cần chương trình chủ. Các phần mềm độc hại thuộc nhóm này gồm Logic bomb, back door …*

*+Các phần mềm độc hại không cần chương trình chủ. Các phần mềm độc hại thuộc nhóm này gồm Worm, zombie, hay Bot …*

**

*-Cách phòng chống:*

*+Ngăn chặn virus lây nhiễm vào hệ thống:*

* *Luôn cập nhật hệ thống để hạn chế các lỗi phần mềm*
* *Sd các biện pháp kiểm soát truy nhập*

*+Khi hệ thống đã bị nhiễm virus:*

* *Phát hiện virus*
* *Nhận dạng virus*
* *Loại bỏ virus*

Câu 5: Anh/chị hãy giải thích các lớp phòng vệ điển hình trong mô hình bảo đảm an toàn hệ thống thông tin có chiều sâu Defence in Depth?

*-Mô hình phòng vệ gồm 3 lớp:* ***Lớp an ninh cơ quan/tổ chức****,* ***lớp an ninh mạng và lớp an ninh hệ thống****. Mỗi lớp trên lại gôm một số lớp con như sau:*

*+Lớp an ninh cơ quan/ tổ chức gồm 2 lớp con:*

1. ***Lớp bảo vệ vật lí*** *có nhiệm vụ kiểm soát các truy cập vật lí đến các trang bị hệ thống và mạng*
2. ***Lớp chính sách và thủ tục*** *bao gồm các quy trình quản lí ATTT, các hướng dẫn vận hành, quản lí hoạt động liên tục và phục hồi sau sự cố.*

*+Lớp an ninh mạng gồm 2 lớp con:*

1. *Lớp bảo vệ vùng hạn chế truy cập cung cấp các biện pháp bảo vệ cho từng phân đoạn mạng*
2. *Các tường lửa, mạng riêng ảo dược triển khai như điểm truy nhập duy nhất đến một phân đoạn mạng*

*+Lớp an ninh hệ thống gồm 4 lớp con:*

1. *Lớp tăng cường an ninh hệ thống đảm bảo việc cài đặt và cấu hình các thành phần trong hệ thống đảm bảo các yêu cầu an toàn*
2. *Lớp quản trị tài khoản người dùng thực hiện kiểm soát truy nhập trên quyền truy và các đặc quyền của người dùng*
3. *Lớp quản lí các bản vá (Patch Manager) có nhiệm vụ cài đặt định kỳ các bản vá an ninh và các bản cập nhật cho hệ thống*
4. *Lớp phát hiện và ngăn chặn phần mềm độc hại (Malware delection and prevention) có nhiệm vụ bảo vệ hệ thống, chống virus và các phần mềm độc hại khác*

Câu 6: Anh/chị hãy giải thích tấn công giả mạo địa chỉ và nêu cách phòng chống ?

*-Tấn công giả mạo địa chỉ IP (KP spoofing):*

*+Là dạng tấn công trong đó kẻ tấn công sử dụng địa chỉ IP giả, thường để đánh lừa máy nạn nhân để vượt qua các hàng rào kiểm soát an ninh.*

*+Nếu router hoặc firewall của mạng không được cấu hình để nhận ra IP giả mạo của mạng LAN nội bộ -> kẻ tấn công có thể thực hiện*

*+Nếu kẻ tấn công giả mạo địa chỉ IP là địa cục bộ của mạng LAN, hắn có thể có nhiều cơ hội đột nhập vào các máy khác trong LAN do chính sách an ninh với các máy trong mạng LAN thường được giảm nhẹ.*

*-Phòng chống: Cách phòng chống hiệu quả nhất là sử dụng kĩ thuật lọc trên firewall, hoặc các router với nguyên tắc lọc: Các gói tin từ mạng ngoài đi vào mạng LAN mà có địa chỉ nguồn là địa chỉ mạng nội bộ của mạng LAN đó thì chúng là các tin giả mạo và phải bị chặn.*

Câu 7: Anh/chị hãy giải thích về các dạng tấn công vào mật khẩu và nêu cách phòng tấn công vào mật khẩu?

*-Tấn công vào mật khẩu (Password attack): Là dạng tấn công nhằm đánh cắp mật khẩu và thông tin tài khoản của người dùng để lạm dụng.*

*-Các dạng tấn công:*

*+Tấn công dựa trên từ điển (Dictionary attacks): Dạng tấn công này khai tác vấn đề người dùng, có xu hướng chọn mật khẩu là các từ đơn giản cho dễ nhớ. Tấn công các từ có tần suất sử dụng cao trong từ điển.*

*+Tấn công vét cạn (Brute force attacks): Dạng vét cạn sử dụng tổ hợp các kí tự và thử tự động. Kẻ tấn công sinh tổ hợp kí tự, sau đó mã hoá với cùng thuật toán mã hoá hệ thống sử dụng rồi so sánh. Nếu 2 bản mã trùng nhau thì tổ hợp kí tự là mật khẩu.*

*-Cách phòng chống:*

*+Chọn mật khẩu đủ mạnh*

*+Định kì thay đổi mật khẩu*

*+Hạn chế trao đổi tên người dùng và mật khẩu trên kênh truyền thông không được mã hoá*

Câu 8: Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên bất thường của hệ thống IDS/IPS?

***-Cơ chế:*** *Dựa trên giả thuyết: Các hành vi đột nhập thường có quan hệ chặn chẽ với các hành vi bất thường.*

*+Quá trình xây dựng và triển khai gồm:*

1. *Xây dựng hồ sơ của đối tượng trong chế độ làm việc bình thường*
2. *Cần giám sát đối tượng trong điều kiện bình thường*
3. *Giám sát hành vi hiện tại của hệ thống và cảnh báo nếu có sự khác biệt giữa hành vi hiện tại và hồ sơ của đối tượng.*

Câu 9: Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên chứ ký của hệ thống IDS/IPS?

***-Cơ chế:*** *Xây dựng cơ sở dữ liệu các chữ ký (dấu hiệu) của các loại tấn công, đột nhập đã biết. Giám sát các hành vi của hệ thống, và cảnh báo nếu phát hiện chữ ký của tấn công, đột nhập.*

Câu 10: Anh/chị hãy giải thích tấn công kiểu Social Engineering và nêu các cách phòng chống ?

*-Tấn công kiểu Social Engineering là dạng tấn công sử dụng các kĩ thuật xã hội để thuyết phục người dùng tiết lộ thông tin truy nhập hoặc các thông tin có giá trị cho kẻ tấn công. ( Giả mạo người có vị trí cao hơn, người được uỷ quyền …)*

*-Cách phòng chống: Cảnh giác với các lời mời hoặc thông báo từ các cuộc gọi, tin nhắn. Cảnh giác với yêu cầu cung cấp thông tin.*

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?

Câu 12: Anh/chị hãy giải thích quan hệ giữa mối đe doạ và lỗ hổng trong hệ thống thông tin và liệt kê các mối đe doạ thường gặp?

*-Mối quan hệ giữa mối đe doạ và lỗ hổng trong HTTT: Các mối đe doạ thường khai thác một hoặc nhiều lỗ hổng bảo mật đã biết để thực hiện các cuộc tấn công phá hoại. Điều này có nghĩa là nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe doạ trở thành hiện thực. Chính vì vậy, mối đe doạ và lỗ hổng bảo mật có quan hệ hữu cơ với nhau.*

*-Liệt kê các mối quan hệ thường gặp:*

1. *Phần mềm độc hại*
2. *Kẻ tấn công ở bên trong*
3. *Kẻ tấn công ở bên ngoài*
4. *Hư hỏng phần cứng hoặc phần mềm*

Câu 13: Anh/chị hãy trình bày về biện pháp điều khiển truy nhập MAC và cho ví dụ?

*-Điều khiển truy nhập bắt buộc (MAC) được định nghĩa là các cơ chế hạn chế truy nhập đến các đối tượng dựa trên hai yếu tố chính:*

*+Tính nhạy cảm của thông tin chứa trong các đối tượng*

*+Sự trao quyền chính thức cho các chủ thể truy nhập các thông tin nhạy cảm.*

*Ví dụ: Quản lí truy cập dữ liệu cá nhân trong y tế.*

Câu 14: Anh/chị hãy trình bày về biện pháp điều khiển truy nhập DAC và cho ví dụ?

*-Điều khiển truy nhập tuỳ chọn (Discretionary Acess Control – DAC) mỗi tài nguyên có các quyền truy cập được quy định bởi người sở hữu hoặc quản trị viên.*

*Ví dụ:*

*+ Trong hệ thống tệp và thư mục của máy tính các nhân, bạn có quyền đọc và chỉnh sửa tất cả tệp và thư mục mà bạn tạo ra.*

*+Trong một mạng chia sẻ, người dùng A có thể được uỷ quyền, quyền đọc một têph những không có quyền ghi.*

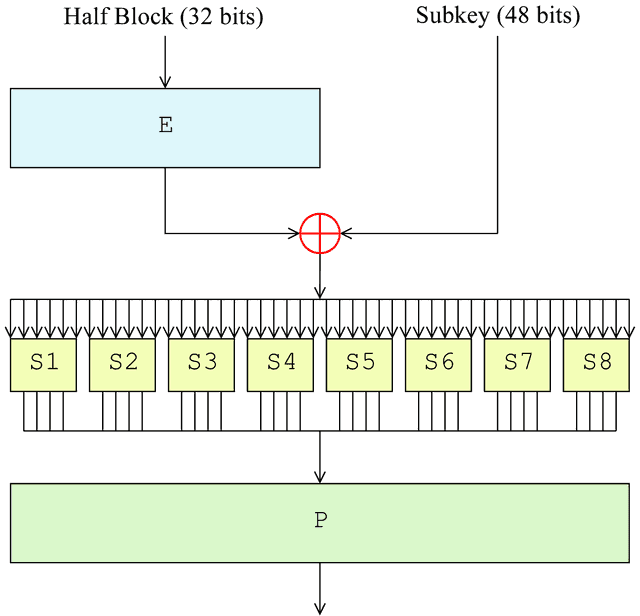
Câu 15: Anh/chị hãy so sánh đặc điểm của hệ mã khoá đối xứng với hệ mã hoá bất đối xứng?

*-Giống: Cả hai đều đóng vai trò quan trọng trong việc bảo đảm bảo mật cho thông tin nhạy cảm và việc thông tin liên lạc trong TG phụ thuộc vào kĩ thuật như ngày nay.*

*-Khác:*

|  |  |  |
| --- | --- | --- |
| *Đặc điểm* | *Bất đối xứng* | *Đối xứng* |
| *Khoá mã hoá* | *Sử dụng 2 khoá khác nhau một khoá để mã hoá dữ liệu và một khoá khác để giải mã nó* | *Sử dụng cùng 1 khoá để thực hiện cae 2 chức năng mã hoá và giải mã* |
| *Thông điệp* | *Thông điệp được mã hoá chỉ có thể được giải mã với khoá riêng của người nhận* | *Người gửi và người nhận thông điệp phải chia sẻ một bí mật gọi là chìa khoá* |
| *Ứng dụng* | *Sử dụng cho các hệ thống mã trong đó nhiêug người dùng có thể cần mã hoá và giải mã tệp hoặc dữ liệu* | *Sử dụng rộng rãi để bảo vệ thông tin trong các hệ thống máy tính hiện đại.* |

Câu 16: Trong hệ mã hoá DES, anh/chị hãy vẽ sơ đồ thuật toán các bước xử lý chính của hệ mã, giải thích sơ đồ ?



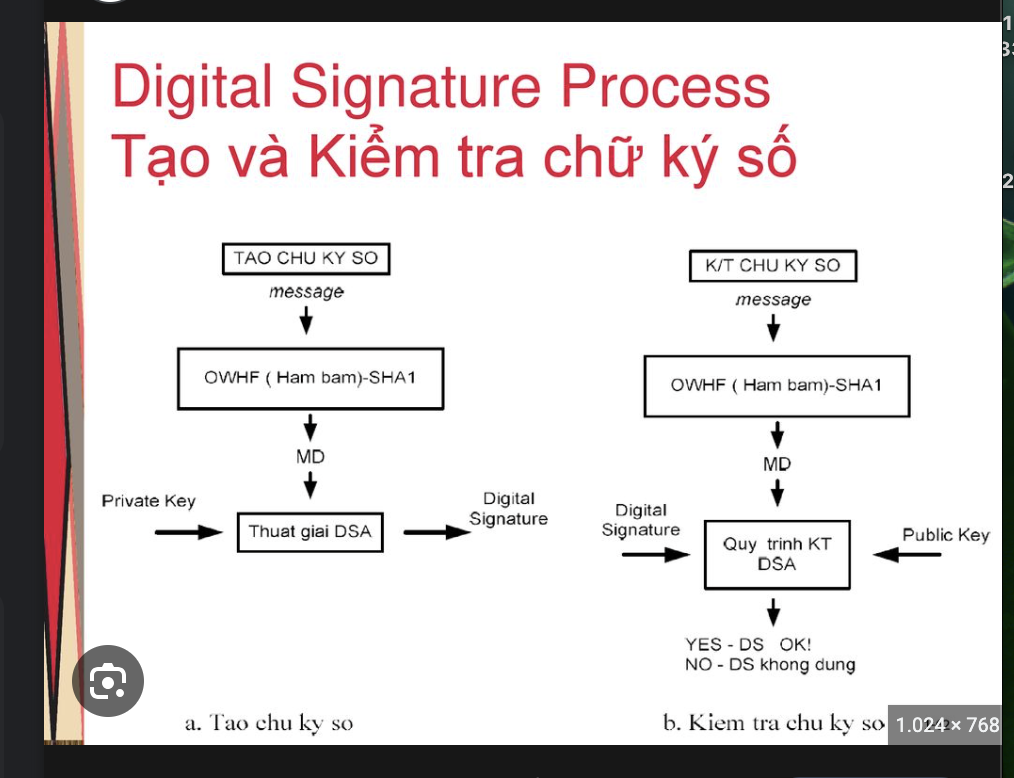
Câu 17: Trong hệ mã DES, Anh/chị hãy vẽ sơ đồ thuật toán các bước sinh khoá phụ của hệ mã, giải thích sơ đồ?

Câu 18: Anh/chị hãy cho biết các thành phần và chức năng của hạ tầng quản lý khoá công khai PKI?

*-PKI là một hệ thống bảo mật được sử dụng để tạo, quản lý và phân phối các khoá công khai và khoá riêng tư, cũng như xác thực danh tính trong môi trường mạng.*

*-Thành phần chức năng của hạ tầng quản lí khoá công khai:*

Câu 19: Anh/chị hãy vẽ sơ đồ quá trình tạo và kiểm tra chữ ký số, giải thích sơ đồ ?



Câu 20: Anh/chị hãy vẽ sơ đồ cấp và sử dụng chứng chỉ số, giải thích sơ đồ?