DANH SÁCH CÂU HỎI ÔN TẬP
HỌC PHẦN AN TOÀN BẢO MẬT THÔNG TIN DOANH NGHIỆP

1. An toàn và bảo mật thông tin là gì? Vì sao an toàn và bảo mật thông tin lại đóng vai trò rất quan trọng trong hoạt động của các doanh nghiệp hiện nay?
2. Trình bày ngắn gọn các xu hướng tấn công được dự đoán trong năm nay ?
3. Mục tiêu của an toàn và bảo mật thông tin trong doanh nghiệp? Vì sao luôn cần xác định mục tiêu trước khi ứng dụng các biện pháp đảm bảo an toàn cho HTTT doanh nghiệp?
4. Các yêu cầu an toàn và bảo mật đối với một hệ thống thông tin trong doanh nghiệp là gì?
5. Những khó khăn doanh nghiệp thường gặp phải khi triển khai các giải pháp an toàn cho HTTT là gì? Lấy ví dụ minh họa
6. Trình bày và giải thích các giải pháp phòng tránh phổ biến mà các doanh nghiệp Việt Nam đang sử dụng hiện nay?
7. Khắc phục sự cố là gì? Vì sao cần có cơ chế khắc phục sự cố trong các HTTT doanh nghiệp? Trình bày và giải thích các nhóm nguy cơ mất an toàn thông tin trong doanh nghiệp hiện nay?
8. Bảo mật hệ thống là gì? Vì sao cần bảo mật hệ thống thông tin? Lấy ví dụ minh họa.
9. Trong các nguy cơ mất an toàn thông tin trong doanh nghiệp thì những nguy cơ nào hiện nay ít được để ý đến nhất? Vì sao?
10. Trình bày các nguy cơ mất an toàn trong HTTT TMĐT? Vì sao các hệ thống thông tin thương mại điện tử lại dễ bị tấn công hơn các hệ thống thông tin khác?
11. Hãy trình bày và giải thích các phương pháp xác định nguy cơ mất an toàn trong các hệ thống thông tin hiện nay? Lấy ví dụ minh họa.
12. Mục tiêu của an toàn và bảo mật thông tin trong doanh nghiệp là gì? Lấy ví dụ minh họa
13. Trình bày các hình thức tấn công thụ động và nêu biện pháp phòng tránh? Trình bày các hình thức tấn công chủ động và nêu biện pháp phòng tránh ?
14. Bảo mật kênh truyền là gì? Vì sao cần bảo mật kênh truyền tin? Có những cơ chế bảo mật kênh truyền nào?
15. Khi máy tính của bạn bị nhiễm các mã độc, bạn cần làm gì để loại bỏ chúng khỏi máy tính? Vì sao càng ngày càng khó phòng tránh những loại mã độc này?
16. Tấn công từ chối dịch vụ là gì? Trình bày đặc trưng của các kiểu tấn công từ chối dịch vụ phổ biến hiện nay? Vì sao hiện nay tấn công từ chối dịch vụ rất khó phòng tránh?
17. Giả sử A đang gửi một thông điệp đã được mã hóa cho B. Các hình thức tấn công thụ động nào sẽ ảnh hưởng đến nội dung thông điệp của A? Hãy giải thích?
18. Tường lửa là gì? Trình bày các loại tường lửa phổ biến hiện nay? Trình bày đặc trưng và xu hướng phát triển của các loại tường lửa hiện nay?
19. Tấn công thụ động là gì ? Tấn công chủ động là gì ? Cho ví dụ minh họa.

20. Phân tích các ưu điểm của bảo mật kênh truyền trong giao dịch thương mại điện tử? Hãy so sánh các giao thức SSL, SET và WEB về khả năng ứng dụng và mức độ an toàn?
21. Bảo mật Website là gì? Trình bày các nguy cơ mất an toàn đối với các loại Website?
22. Tường lửa phần mềm là gì? Tại sao cần cài đặt tường lửa phần mềm cho máy tính cá nhân của bạn?
23. Mã hóa dữ liệu là gì? Khi nào cần mã hóa dữ liệu? Trình bày các ứng dụng của mã hóa dữ liệu.
24. So sánh 3 giao thức bảo mật kênh truyền SSL, SET và WEP trên 2 tiêu chí: Tính phổ dụng và độ an toàn khi sử dụng chúng?
25. Phân quyền người dùng là gì? Vì sao trong HTTT doanh nghiệp cần phân quyền người dùng?
26. Chứng thực điện tử là gì? Trình bày và giải thích đặc điểm của các loại chứng thực điện tử được sử dụng phổ biến hiện nay? Chứng thực điện tử được xây dựng dựa trên hệ mã hóa nào? Lấy ví dụ minh họa
27. Thế nào là truyền tin an toàn? Trình bày mô hình truyền tin an toàn?
28. Trình bày các ứng dụng của mã hóa khóa công khai hiện nay? Lấy ví dụ minh họa. Phân tích những lợi ích của mã hóa dữ liệu?
29. Trình bày sơ đồ mã hóa khóa đối xứng và ứng dụng của chúng? Lấy ví dụ minh họa
30. Chữ ký điện tử là gì? Trình bày các ứng dụng của chữ ký điện tử? Trình bày các đặc điểm của chữ ký điện tử? Lấy ví dụ minh họa
31. Giả sử A muốn gửi một thông điệp cho B trên một kênh truyền biết trước. Để tránh thông điệp bị tấn công chủ động thì A cần các biện pháp phòng tránh nào? Giải thích?
32. Khi nào một thuật toán mã hóa được coi là an toàn vô điều kiện và an toàn tính toán?
33. Bạn đang sử dụng một máy tính cá nhân (Personal Computer - PC) trong công việc.
    a. Hãy liệt kê và phân tích các nguy cơ mất an toàn đối với các thông tin trong máy tính đó?
    b. Hãy liệt kê và phân tích các lỗ hổng bảo mật có thể có của máy tính đó?
    c. Hãy đề xuất và giải thích các giải pháp đảm bảo an toàn thông tin cho máy tính đó.
    d. Hãy đề xuất và giải thích các giải pháp phòng tránh các lỗ hổng bảo mật cho máy tính đó.
34. Bạn đang sử dụng một máy tính tại văn phòng làm việc có kết nối mạng Internet.
    a. Hãy liệt kê và phân tích các nguy cơ mất an toàn đối với các thông tin trong máy tính đó?
    b. Hãy liệt kê và phân tích các lỗ hổng bảo mật có thể có của máy tính đó?
35. Bạn đang sử dụng một tài khoản email tại văn phòng làm việc có kết nối mạng Internet để trao đổi thông tin với khách hàng.
    a. Hãy liệt kê và phân tích các nguy cơ mất an toàn có thể gặp phải đối với tài khoản email đó?

b. Hãy đề xuất và giải thích các biện pháp đảm bảo an toàn khi sử dụng tài khoản email đó?
c. Hãy trình bày các kiểu mã hóa có thể sử dụng để tạo mật khẩu cho email đó đảm bảo tính an toàn khi sử dụng?

36. Công ty của bạn đang sử dụng một Website để quảng bá và giới thiệu thông tin các sản phẩm đến đối tác và khách hàng.
    a. Hãy liệt kê và phân tích các nguy cơ mất an toàn có thể gặp phải đối với Website đó.
    b. Hãy liệt kê và phân tích các lỗ hổng bảo mật có thể có đối với Website đó.
    c. Hãy trình bày các biện pháp đảm bảo an toàn cho Website đó.
    d. Hãy trình bày các cách thức phân quyền người dùng trên Website đó.
37. Công ty của bạn đang sử dụng một mạng LAN bao gồm 200 máy tính kết nối với nhau để trao đổi thông tin nội bộ của doanh nghiệp.
    a. Hãy trình bày và phân tích các nguy cơ mất an toàn đối với mạng LAN đó.
    b. Hãy trình bày và phân tích các lỗ hổng có thể gặp phải đối với mạng LAN đó.
    c. Hãy trình bày và giải thích các giải pháp đảm bảo an toàn cho mạng LAN đó.
    d. Hãy đề xuất và giải thích các giao thức truyền thông đảm bảo an toàn cho mạng LAN trên.
    e. Hãy đề xuất và giải thích một quy trình bảo mật nhiều lớp và đa phương thức để bảo mật cho mạng LAN trên.
    f. Hãy đề xuất và giải thích một quy trình bảo mật nhằm phòng tránh tấn công vào hệ thống lưu trữ dữ liệu của mạng LAN trên.
38. Công ty của bạn đang sử dụng một số phần mềm ứng dụng (Applications) hỗ trợ cho các hoạt động kinh doanh của tổ chức.
    a. Hãy liệt kê và phân tích các nguy cơ mất an toàn có thể gặp phải của các ứng dụng đó.
    b. Hãy liệt kê và phân tích các lỗ hổng bảo mật có thể có của các ứng dụng đó.
    c. Hãy trình bày và giải thích các biện pháp đảm bảo an toàn cho các ứng dụng đó.
    d. Hãy trình bày và giải thích các biện pháp phòng tránh cho các lỗ hổng bảo mật có thể có của các ứng dụng đó.
39. Công ty của bạn đang sử dụng một hệ quản trị cơ sở dữ liệu để quản trị cơ sở dữ liệu cho tổ chức.
    a. Hãy liệt kê và phân tích các nguy cơ mất an toàn có thể gặp phải đối với cơ sở dữ liệu của tổ chức.
    b. Hãy liệt kê và phân tích các lỗ hổng có thể có đối với hệ thống quản trị cơ sở dữ liệu của tổ chức.
    c. Hãy trình bày và giải thích các biện pháp đảm bảo an toàn cho cơ sở dữ liệu của tổ chức.

d. Hãy trình bày và phân tích các quyền người dùng có thể sử dụng đối với hệ thống quản trị cơ sở dữ liệu đó.

40. Nhân viên trong công ty đang sử dụng nhiều tài khoản bao gồm tên tài khoản và mật khẩu để đăng nhập trên nhiều ứng dụng khác nhau của tổ chức.
    a. Hãy liệt kê và phân tích các nguy cơ mất an toàn có thể gặp phải đối với các tài khoản đó.
    b. Hãy trình bày và giải thích các biện pháp phòng tránh các nguy cơ cho người dùng khi sử dụng các tài khoản đó.
41. Công ty của bạn có sử dụng dịch vụ page/account trên một số trang mạng xã hội để giới thiệu, quảng bá các sản phẩm và dịch vụ tới khách hàng.
    a. Hãy liệt kê và phân tích các nguy cơ mất an toàn có thể gặp phải đối với việc sử dụng các dịch vụ đó.
    b. Hãy trình bày và giải thích các giải pháp đảm bảo an toàn cho công ty khi sử dụng các dịch vụ đó.
42. Giả sử Alice muốn trao đổi thông tin với Bob nhưng không muốn người khác xem được thông tin cần trao đổi. Theo bạn, Alice cần dùng các biện pháp nào để trao đổi thông tin với Bob cho an toàn? Hãy giải thích ?
43. Công ty của bạn có sử dụng dịch vụ ngân hàng trực tuyến e-banking để giao dịch và thanh toán cho nhà cung cấp và khách hàng.
    a. Hãy trình bày và giải thích các giải pháp đảm bảo an toàn cho công ty khi sử dụng các dịch vụ ngân hàng trực tuyến này.
    b. Hãy liệt kê và phân tích các nguy cơ mất an toàn cho công ty khi sử dụng các dịch vụ ngân hàng trực tuyến này.
    c. Hãy xác định và phân tích các lỗ hổng có thể gặp phải của cho công ty khi sử dụng các dịch vụ ngân hàng trực tuyến này.
44. Khách hàng của bạn có sử dụng dịch vụ ngân hàng trực tuyến e-banking để thanh toán khi giao dịch với các website thương mại điện tử.
    a. Hãy xác định và phân tích các lỗ hổng có thể gặp phải của khách hàng khi họ sử dụng các dịch vụ ngân hàng trực tuyến trên thiết bị di động?
    b. Hãy xác định và phân tích các nguy cơ có thể gặp phải của khách hàng khi họ sử dụng các dịch vụ ngân hàng trực tuyến trên máy tính điện tử?
45. Hãy so sánh ưu điểm và nhược điểm của máy tính điện tử với điện thoại di động trên phương diện an toàn thông tin, khi thực hiện các giao dịch thanh toán trực tuyến.
46. Giả sử A muốn gửi một thông điệp cho B trên một kênh truyền biết trước. Để tránh thông điệp bị tấn công bị động thì A cần các biện pháp phòng tránh nào? Giải thích?
47. Hãy so sánh ưu điểm và nhược điểm của các hệ mã hóa hiện đại? Vì sao các hệ mã hóa đều không thể thỏa mãn an toàn vô điều kiện? Hãy giải thích

BÀI TẬP:

Ôn tập các hệ mã hóa đối xứng cổ điển

- Hệ mã hóa cộng Ceasar
- Hệ mã hóa nhân
- Hệ mã hóa tích hợp Cộng và nhân, Nhân và Cộng
- Hệ mã hóa Vigenere
- Hệ mã hóa khóa tự động
- Hệ mã hóa hàng rào
- Hệ mã hóa hàng

Ghi nhớ thuật toán mã hóa bất đối xứng RSA

- Giai đoạn sinh cặp khóa bí mật và công khai
- Giai đoạn mã hóa
- Giai đoạn giải mã