Đề cương ôn tập cho sinh viên khóa 16

Lớp Đảm bảo và An toàn thông tin

Giáo viên: Vũ Đình Phái

BM ATTT - Khoa CNTT -HVKTQS

Bài tập 4đ, Lý thuyết 6 đ

Thi vấn đáp

Lý thuyết

Phần 1: Lý thuyết đảm bảo an toàn thông tin

1. Tại sao vấn đề bảo mật thông tin lại là vấn đề quản lý?
2. Việc triển khai công nghệ mạng có tạo ra ít hoặc nhiều rủi ro cho doanh nghiệp sử dụng công nghệ thông tin? Tại sao?
3. Tống tiền thông tin là gì? Mô tả cách tấn công như thế có thể gây ra tổn thất, nêu ví dụ.
4. Tại sao nhân viên lại là một trong những mối đe dọa lớn nhất đối với an ninh thông tin?
5. Nhận thức của hacker đã thay đổi như thế nào trong những năm gần đây? Hồ sơ của một hacker hôm nay là gì?
6. Sự khác biệt giữa một hacker có kỹ năng và một hacker không có kỹ năng (ngoài các cấp độ kỹ năng) là gì?
7. Các loại phần mềm độc hại khác nhau là gì? Trojan horses khác virus và worm ở điểm nào?
8. Nêu sự liên quan giữa các nhóm chính sách, tiêu chuẩn, chỉ dẫn. Cho một ví dụ minh họa về sự liên quan đó.
9. Mục tiêu của an toàn bảo mật thông tin. Đưa ra ví dụ việc đảm bảo các mục tiêu của an toàn và bảo mật thông tin.
10. Ý nghĩa của phân lớp tài sản. Nêu sự liên quan của phân lớp tài sản với chính sách quản lý tài liệu, điều khiển truy xuất.
11. Ý nghĩa điều khiển truy xuất. Các nhân tố xác thực người dùng. Lý do cần có sự kết hợp giữa các nhân tố xác thực.

12. Ý nghĩa bảo mật vật lý, ví dụ chính sách bảo mật vật lý
13. Ý nghĩa của phân tích nguy cơ, tiến trình phân tích quản lý nguy cơ
14. Ý nghĩa kế hoạch công việc liên tục, sự liên quan của quá trình phân tích tác động công việc và các bước
15. Nêu lý do của vì sao phải thiết lập chính sách, tiêu chuẩn, chỉ dẫn về an toàn và đảm bảo thông tin trong doanh nghiệp.
16. Sự tương ứng của phân tích nguy cơ và quá trình phát triển hệ thống? Vòng đời của bảo mật thông tin?
17. Tiêu chuẩn ISO 27000 là gì, ý nghĩa của việc áp dụng tiêu chuẩn này. Sự liên quan giữa tiêu chuẩn và chất lượng sản phẩm của hệ thống.

Phần 2: Câu hỏi về phần kỹ thuật liên quan đến an toàn và bảo mật hệ thống thông tin

1. Điều khiển truy cập bắt buộc, tùy quyền, xác thực, ủy quyền là gì
2. Firewall là gì, phần loại firewall
3. Hệ thống IDS, IPS là gì
4. Phân loại mạng không dây, cơ chế xác thực, lọc địa chỉ MAC, mã hóa sử dụng trong mạng không dây
5. Nêu một số thuật toán mã hoá cổ điển, phân tích khả năng áp dụng mô hình cho mã hoá dữ liệu lưu trữ và mã hoá dữ liệu trên đường truyền.
6. Khác nhau giữa mã hoá đối xứng và mã hóa bất đối xứng. Nguyên lý của hàm băm, khả năng sử dụng hàm băm trong bảo vệ dữ liệu và các hệ thống ứng dụng
7. Cơ sở của mã hoá công khai RSA, phân tích khả năng sử dụng mã hoá RSA để lưu trữ dữ liệu trên hệ thống máy tính, truyền dữ liệu trên mạng máy tính.
8. Phân tích sự khác biệt mã hóa cổ điển và mã công khai, khả năng kết hợp giữa hai loại khóa trong truyền tin?
9. Trình bày mô hình chữ ký số. Sự cần thiết của triển khai mô hình chữ ký số trong giao dịch điện tử ở Việt Nam. Trình bày hiểu biết về hiện trạng mô hình chữ ký số ở Việt Nam.

10. Tấn công mạng, các bước tấn công mạng là gì, trinh sát, quét cổng, dò tìm lỗ hổng….
11. Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Port scaning attack, Avesdropping attack, IP spoofing attack
12. Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Hijacking attack, Replay attack, Man-in-the-middle attack
13. Tấn công SQL injection, tràn bộ đệm, chéo trang – cross page attack? Giải pháp phòng chống?
14. Tấn công DoS, DDoS nguyên lý và khả năng phòng chống?
15. Khác nhau giữa virus, worm, trojan, back door, rookit
16. Phương pháp phân tích mã độc tính, động là gì
17. Khả năng bảo vệ hệ thống của trình quét virus và firewall
18. IPSec, VPN khả năng bảo vệ thông tin trên đường truyền
19. Các hệ thông sau dùng để làm gì

    Hệ thống tấn công BPS, Công cụ Burpsuit, Hệ thống Flowmon, Hệ thống Sonicwall TZ400 , Hệ thống addnet , Hệ thống Logrythm

Bài tập:

1. Bài tập về mã hóa cổ điển, RSA
2. Bài tập đánh giá rủi ro, tính lợi ích chi phí và đưa ra các chính sách với từng rủi ro cụ thể
3. Bài tập về cấu hình firewall, chính sách mật khẩu, xem log trên window