Chương 1:

Câu 1: What is the OSI security architecture ?

Kiến trúc bảo mật OSI là khuôn khổ mà cung cấp một cách có hệ thống quy đị nh các yêu cầu cho bảo mật và mô tả đặc tính phương pháp tiếp cận để đáp ứng những yêu cầu.

Tài liệu này đị nh nghĩa các cuộc tấn công an ninh, cơ chế, dị ch vụ, và các mối quan hệ giữa các loại

Câu 2: What is the difference between passive and active security threats?

Sol : Các cuộc tấn công thụ động phải thực hiện với nghe trộm, hoặc giám sát, truyền đi. Thư điện tử, chuyển file, và trao đổi giữa client / server(Electronic mail, file transfers, and client/server exchanges) là những ví dụ của truyền có thể được theo dõi.

Các cuộc tấn công chủ động : bao gồm những việc như sửa đổi các dữ liệu được truyền và nỗ lực để đạt được quyền truy cập trái phép vào hệ thống máy tính.

Câu 3: List and briefly define categories of passive and active security attacks.

Sol :

các cuộc tấn công thụ động: release nội dung tin nhắn và phân tích lưu lượng.

các cuộc tấn công chủ động: giả danh (masquerade), phát lại (replay), sửa đổi các thông điệp (modification messages), và từ chối dị ch vụ (denial of service).

Câu 4 : liệt kê và đị nh nghĩa ngắn gọn các loại dị ch vụ an ninh ?

+ Authentication(Sự xác thực) : đảm bảo rằng giao tiếp đối tượng được tuyên bố.

+ Access Control (Kiểm soát truy cập): Phòng chống việc sử dụng trái phép tài nguyên

+ Data Confidentiality(Bảo mật dữ liệu) – bảo vệ dữ liệu không bị tiết lộ trái phép.

+ Data Integrity(Toàn vẹn dữ liệu)- Đảm bảo rằng dữ liệu nhận được khi gửi bởi một đơn vị có thẩm quyền.

+ Non-Repudiation(Không thoái thác) - bảo vệ chống lại sự từ chối của một trong các bên trong một giao tiếp

+ Availability – tài nguyên truy cập / hữu dụng

Câu 5 : liệt kê và đị nh nghĩa ngắn gọn loại **cơ chế bảo mật**? (security mechanisms)

 Security mechanisms: Được biết đến như là kiểm soát (control).

Security mechanisms: Tính năng được thiết kế để phát hiện(detect), ngăn chặn(prevent), hoặc phục hồi (recover) từ một cuộc tấn công an ninh.

 Không có cơ chế duy nhất mà sẽ hỗ trợ tất cả các dị ch vụ cần thiết

- Tuy nhiênmột yếu tố đặc biệt làm nền tảng cho rất nhiều các cơ chế bảo mật được sử dụng: các kỹ thuật mã hóa

Specific SecurityMechanisms (Cơchế bảo mật cụ thể)

- Encipherment (Mã hóa)
- Digitalsignatures (chữký số)
- Accesscontrols (kiểm soát truy cập)
- Dataintegrity (Toàn vẹn dữliệu)
- Authenticationexchange (Trao đổi xác thực)
- Trafficpadding (đệm lưu lượng)
- Routingcontrol (Kiểm soát định tuyến)
- Notarization (Công chứng)

Pervasive SecurityMechanisms (Cơchế bảo mật phổbiến)

- trustedfunctionality (chức năng đáng tin cậy)
- securitylabels (nhãn an ninh)
- eventdetection (phát hiện sựkiện)
- security auditttrails (con đường kiểm tra an ninh)
- securityrecovery (phục hồi an ninh)

cuu duong than cong. com

Chương 9 Intruder (Kẻ xâm nhập)

Câu 1: Liệt kê và đị nh nghĩa ngắn gọn 3 loại (three classes) kẻ xâm nhập ? Sol:

+ Masquerader /mæs-kə-´reid/(Kẻ giả danh): (Outsider)

Là một cá nhân không có quyền sử dụng máy tính của người sử dụng hợp pháp , đó là người thâm nhập kiểm soát truy cập của hệ thống để khai thác tài khoản của người sử dụng hợp pháp.

+ Mis'feasor /mis-'fi:-sə/(Kẻ lạm dụng quyền): (Insider)

Là người dùng hợp pháp ,là người có thể truy cập dữ liệu, chương trình, hoặc tài nguyên mà truy cập như vậy là không được phép, hoặc đó là người được ủy quyền để truy cập nhưng lợi dụng đặc quyền của mình.

+ Clandestine/klæn-'des-tin/ user: (Người dùng giấu mặt):(either outsider or insider)

Là một cá nhân nắm quyền kiểm soát giám sát của hệ thống và sử dụng điều khiển này để trốn tránh sự kiểm tra và truy cập điều khiển hoặc để ngăn chặn thu thập kiểm tra.

Câu 2: Hai kỹ thuật để bảo vệ tập tin mật khẩu là gì ?

+ One-way function : Mã hóa mật khẩu rồi lưu vào hệ thống (hệ thống chỉ lưu mật khẩu đã được mã hóa) -> khi người dùng nhập pass -> hệ thống mã hóa pass đó rồi mới so sánh với pass đã lưu .

+Access control : Truy cập vào các tập tin mật khẩu được giới hạn ở một hoặc một số rất ít các tài khoản

Câu 3 : Ba lợi ích mà có thể được cung cấp bởi một hệ thống phát hiện xâm nhập là gì ? (intrusion detection system)

1. Nếu một sự xâm nhập được phát hiện một cách nhanh chóng đầy đủ, kẻ xâm nhập có thể được nhận biết và bị đẩy ra khỏi hệ thống trước khi bất kỳ thiệt hại được thực hiện hoặc bất kỳ dữ liệu bị phá hoại. Thậm chí nếu phát hiện là không đủ kị p thời nhằm chặn trước những kẻ xâm nhập, sớm hơn rằng sự xâm nhập được phát hiện, trừ các khoản thiệt hại và phục hồi nhanh hơn mà có thể đạt được.

2. Một hệ thống phát hiện xâm nhập có hiệu quả có thể phục vụ như một vật cản, do đó có thể hành động để ngăn chặn sự xâm nhập.

3. Phát hiện xâm nhập cho phép thu thập thông tin về các kỹ thuật xâm nhập có thể được sử dụng để tăng cường cơ sở phòng chống xâm nhập.

Câu 4 : Sự khác biệt giữa phát hiện bất thường dựa theo thống kê và phát hiện xâm nhập dựa trên luật là gì ? (statistical anomaly detection and rule-based intrusion)