CÂU HỎI ÔN TẬP CUỐI KỲ
MÔN: BẢO MẬT CƠ SỞ DỮ LIỆU
------o0o------

1) Sinh viên hãy trình bày về bài toán xác thực (Audentication) và uỷ quyền (Authorization) trong lĩnh vực bảo mật cơ sở dữ liệu. Trình bày các phương pháp xác thực và uỷ quyền hiện nay đang sử dụng? Mô tả 1 phương pháp mà bạn cho là tối ưu nhất hiện nay? Giải thích vì sao bạn chọn phương pháp này? Cho ví dụ minh hoạ.

2) Sinh viên hãy giải thích vì sao điều khiển truy cập tùy quyền không kiểm soát được luồng thông tin. Cho ví dụ minh hoạ //Hướng dẫn: xem ví dụ về cách tấn công Trojan

3) Sinh viên hãy trình bày về bài toán kiểm toán truy cập (Auditing) trong lĩnh vực bảo mật cơ sở dữ liệu. Cho ví dụ minh hoạ

4) Giải thích tính "tùy ý" trong mô hình điều khiển truy cập tùy ý? Trong mô hình điều khiển truy cập tùy ý, những loại người dùng nào có quyền phân quyền/thu hồi quyền hạn? Trong mô hình điều khiển truy cập tùy ý, tại sao ưu điểm là tính linh hoạt, tính dễ dàng trong quản lt1 quyền truy cập. Cho ví dụ minh hoạ?

5) Tại sao khi cài đặt, người ta sử dụng danh sách khả năng thay thế cho cấu trúc ma trận phân quyền? Cho ví dụ minh hoạ

6) Giải thích tính "bắt buộc" trong mô hình điều khiển truy cập bắt buộc? Trong mô hình điều khiển truy cập bắt buộc, tại sao nó ít được vận dụng trong thực tế? Tại sao mô hình điều khiển truy cập bắt buộc được áp dụng trong môi trường quân đội. Trong mô hình điều khiển truy cập bắt buộc, tại sao nó ít mang tính nghiêm ngặt/khắc khe?

7) Ý tưởng trọng tâm của mô hình RBAC là gì? Vì sao RBAC hỗ trợ nguyên tắc bảo mật: đặc quyền ít nhất (Least Privilege)? Vì sao RBAC hỗ trợ nguyên tắc bảo mật: sự tách biệt các nhiệm vụ (Separation of duties). Vì sao RBAC hỗ trợ nguyên tắc bảo mật: trừu tượng hóa dữ liệu (Data Abstraction).

8) Điểm đặc trưng của mô hình Hierarchical RBAC là gì? Điểm đặc trưng của mô hình Static Separation of Duty Relations là gì? Điểm đặc trưng của mô hình Dynamic Separation of Duty Relations là gì? Ứng dụng của từng mô hình? Cho ví dụ minh hoạ

9) So sánh điểm giống/khác nhau giữa hai khái niệm kế thừa vai trò tổng quát (General Role Hierarchies) và kế thừa vai trò bị giới hạn (Limited Role Hierarchies).

10) Trong mô hình RBAC, xung đột (Conflit) quyền hạn là gì? Bạn hãy nêu một chiến lược (strategy) hoặc giải pháp (solution) giải quyết xung đột. Cho ví dụ minh hoạ

11) Nêu các phương pháp bảo mật CSDL NoSQL mà bạn biết. Trình bày 1 phương pháp mà bạn nghĩ là tối ưu nhất? Giải thích tại sao bạn chọn phương pháp này

12) Trình bày các kiểu tấn công vào CSDL hiện nay? Hậu quả của các kiểu tấn công này? Nêu những rủi ro mà Doanh nghiệp sẽ gặp phải trong bảo mật CSDL hiện nay? Nêu ví dụ minh hoạ. Mô tả các giải pháp phòng chống để ngăn ngừa các kiểu tấn công mà bạn đã trình bày.

13) Bạn hãy trình bày và mô tả các cơ chế mã hoá trong SQL Server sau:

- Transact-SQL functions

- Asymmetric keys
- Symmetric keys
- Certificates
- Transparent Data Encryption

14) Trình bày tổng quan về việc sử dụng SQL Server Audit (Overview of Using SQL Server Audit) Nêu các thành phần của SQL Server Audit? SQL Server Audit thường dùng trong những trường hợp nào? Cho ví dụ minh hoạ?

15) Bạn hiểu thế nào về **Database Mirroring**, **logshipping và replication**. Cho ví dụ minh hoạ.

16) Cho bảng dữ liệu SINHVIEN(**masv**, hodem, ten, sodienthoai, diachi, sotaikhoan) chứa nhiều dữ liệu phục vụ hệ thống phần mềm đã được vận hành nhiều năm. Do nhu cầu nâng cấp bảo mật bằng phương pháp mã hóa dữ liệu sử dụng giải pháp được Microsoft SQL Server cung cấp sẵn, thực hiện các yêu cầu sau đây:
    a. Tạo bảng SINHVIEN_MAHOA để chứa dữ liệu được chuyển đổi từ bảng SINHVIEN, viết câu lệnh chuyển đổi dữ liệu bản rõ từ bảng SINHVIEN sang dữ liệu bản mã và lưu trữ vào bảng SINHVIEN_MAHOA.
    b. Với bảng dữ liệu SINHVIEN_MAHOA chứa dữ liệu đã được mã hóa, trình bày giải pháp được thực hiện ở tầng cơ sở dữ liệu sao cho tầng ứng dụng (app) ít sửa đổi nhất? Cho ví dụ với các trường hợp xem, thêm, xóa, sửa dữ liệu sinh viên?

17) Giải thích mô hình Audit sau: