

Course 2787 — Instructor-led

Course Length: 2 days

Prerequisites:

Before attending this class, students must have:

- Have basic knowledge of security protocols and how they work. For example, Windows NT LAN Manager (NTLM) or Kerberos.
- Have basic knowledge of public key infrastructure (PKI) systems. For example, how public and private keys work, strengths and weaknesses, and what they are used for.
- Have working knowledge of network architectures and technologies. For example, how a firewall works, how IPSec works in a networking context, and common vulnerability points.
- Have working knowledge of Active Directory directory service. For example, security models, policies, group policy objects (GPOs), and organizational units (OUs).
- Be able to design a database to third normal form (3NF) and know the tradeoffs when backing out of the fully normalized design (denormalization) and designing for performance and business requirements in addition to being familiar with design models, such as Star and Snowflake schemas.
- Have strong monitoring and troubleshooting skills.
- Have experience creating Microsoft Office Visio drawings or have equivalent knowledge.
- Have strong knowledge of the operating system and

platform. That is, how the operating system integrates with the database, what the platform or operating system can do, interaction between the operating system and the database.

- Have basic knowledge of application architecture. That is, different methods of implementing security in an application, how applications can be designed in three layers, what applications can do, the interaction between applications and the database, and interactions between the database and the platform or operating system.
- Have knowledge about network security tools. For example, sniffer and port scanning. Must understand how they should be used.
- Be able to use patch management systems.
- Have knowledge of common attack methods. For example, buffer overflow, and replay attacks.
- Be familiar with SQL Server 2005 features, tools, and technologies.
- Have a Microsoft Certified Technology Specialist: Microsoft SQL Server 2005 credential or equivalent experience.

In addition, it is recommended, but not required, that students have completed:

- Course 2778: Writing Queries Using Microsoft SQL Server 2005 Transact-SQL.
- Course 2779: Implementing a Microsoft SQL Server 2005 Database.
- Course 2780: Maintaining a Microsoft SQL Server 2005 Database.

Course Outline

Module 1: Introduction to Designing SQL Server Security

This module introduces the principles and methodology of designing SQL Server security. This module also explains the benefits of having a security policy in place and the process of creating a security policy. In addition, this module teaches you the importance of monitoring the security of SQL Server.

Lessons

- Principles of Database Security
- Methodology for Designing a SQL Server Security Policy
- Monitoring SQL Server Security

Module 2: Designing a SQL Server Systems Infrastructure Security Policy

This module provides the guidelines for implementing server-level security using authentication methods. This module also provides the knowledge required to develop a Microsoft Windows server-level security policy. To enable you to do this, this module provides the guidelines to create password policy and determine service accounts permissions. In addition, this module explains how to select an appropriate encryption method to develop a secure communication policy. This module also explains the monitoring standards for SQL Server.

Lessons

- Integrating with Enterprise Authentication Systems
- Developing Windows Server-Level Security Policies
- Developing a Secure Communication Policy
- Defining SQL Server Security Monitoring Standards

Designing Security for Microsoft SQL Server 2005

Course 2787 — continued

Lab 2A: Designing a SQL Server Systems Infrastructure Security Policy

- Developing Microsoft Windows Server-Level Security Policies
- Developing a Secure Communication Policy
- Integrating SQL Server Security Within the Active Directory Environment
- Integrating SQL Server Security With Firewall Configurations
- Discussing Systems Infrastructure Security Integration

Lab 2B: Creating an Infrastructure Security Inventory

- Auditing the SQL Server Logins
- Auditing the Windows Local Password Policy
- Auditing SQL Server Service Accounts
- Monitoring Security at the Enterprise and Server Levels

Module 3: Designing Security Policies for Instances and Databases

This module explains how to design SQL Server instance-level, database-level, and object-level security policies. This module teaches the security monitoring standards for instances and databases.

Lessons

- Designing an Instance-Level Security Policy
- Designing a Database-Level Security Policy
- Designing an Object-Level Security Policy
- Defining Security Monitoring Standards for Instances and Databases

Lab 3A: Designing Security Policies for Instances and Databases

- Designing an Instance-Level Security Policy
- Designing a Database-Level Security Policy
- Designing an Object-Level Security Policy
- Discussing Database Security Exceptions

Lab 3B: Validating Security Policies for Instances and Databases

- Auditing Existing Server Logins
- Auditing SQL Server Roles Membership
- Analyzing Existing Object Permissions
- Monitoring Security at the Instance and Database Level

Module 4: Integrating Data Encryption into a Database Security Design

This module provides the guidelines and considerations for security data using encryption and certificates. This

module also describes various data encryption policies. Finally, this module shows how to determine a key storage method.

Lessons

- Securing Data by Using Encryption and Certificates
- Designing Data Encryption Policies
- Determining a Key Storage Method

Lab 4: Integrating Data Encryption into a Database Security Design

- Selecting a Data Security Method
- Designing a Data Encryption Security Policy
- Selecting a Key Storage Method

Module 5: Designing a Security Exceptions Policy

This module provides guidelines for gathering business and regulatory requirements and comparing them with existing policy. This module also covers how to determine the exceptions and their impact on security.

Lessons

- Analyzing Business and Regulatory Requirements
- Determining the Exceptions and their Impact

Lab 5: Designing a Security Exceptions Policy

- Identifying Variations from the Security Policy
- Obtaining Approval of the Security Policy
- Discussing the Results of Policy Approval Presentations

Module 6: Designing a Response Strategy for Threats and Attacks

This module provides guidelines to respond to virus and worm attacks, denial-of-service attacks, and injection attacks.

Lessons

- Designing a Response Policy for Virus and Worm Attacks
- Designing a Response Policy for Denial-of-Service Attacks
- Designing a Response Policy for Internal and SQL Injection Attacks

Lab 6: Designing a Response Strategy for Threats and Attacks

- Designing a Response Policy for Virus and Worm Attacks
- Designing a Response Policy for Denial-of-Service Attacks
- Designing a Response Policy for Internal Attacks
- Validating a Security Policy