

ITMT 1074

Course Syllabus

1. Name of Course: Designing Security for Microsoft SQL Server 2005

2. Number of Clock Hours: 16

3. Course Description:

This course enables database administrators who work with enterprise environments to design security for database systems using Microsoft SQL Server 2005. The course emphasizes that students should think about the whole environment, which includes business needs, regulatory requirements, network systems, and database considerations during design. Students will also learn how to monitor security and respond to threats. Prerequisites: ITMT 1073 Designing a Microsoft SQL Server 2005 Infrastructure.

4. Course Objectives

Explain the principles of SQL Server security.
Describe the methodology to design a SQL Server security policy.
Explain the importance of monitoring SQL Server security.
Integrate SQL Server security with enterprise-level authentication systems.
Develop Windows server-level security policies.
Develop a secure communication policy.
Define security monitoring standards for SQL Server at the enterprise and server level.
Design a SQL Server instance-level security policy.
Design a database-level security policy.
Design an object-level security policy.
Define security monitoring standards for instances and databases.
Secure data by using encryption and certificates.
Design data encryption policies.
Determine a key storage method.
Analyze business and regulatory requirements.
Determine the exceptions and their impact on security.
Design a response policy for virus and worm attacks.
Design a response policy to handle the denial-of-service attacks.
Design a response policy to prevent internal and SQL injection attacks.

5. Rationale:

Upon completion of this course, students will have a better understanding of Microsoft SQL Server 2005, a power database system.

6. Required Materials:

Microsoft Official Curriculum, MOC 2787, included.

7. Evaluation

Those who participate in class discussions, complete course lab work, and miss no more than three class meetings will be awarded 1.6 continuing education units.

8. 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

After completing this module, students will be able to:

- Explain the principles of SQL Server security.
- Describe the methodology to design a SQL Server security policy.
- Explain the importance of 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

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

After completing this module, students will be able to:

- Integrate SQL Server security with enterprise-level authentication systems.
- Develop Windows server-level security policies.
- Develop a secure communication policy.
- Define security monitoring standards for SQL Server at the enterprise and server level.

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

After completing this module, students will be able to:

- Design a SQL Server instance-level security policy.
- Design a database-level security policy.
- Design an object-level security policy.

- Define security monitoring standards for instances and databases.

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

After completing this module, students will be able to:

- Secure data by using encryption and certificates.
- Design data encryption policies.
- Determine 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

After completing this module, students will be able to:

- Analyze business and regulatory requirements.

- Determine the exceptions and their impact on security.

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

After completing this module, students will be able to:

- Design a response policy for virus and worm attacks.
- Design a response policy to handle the denial-of-service attacks.
- Design a response policy to prevent internal and SQL injection attacks.