

Designing Security for Microsoft Networks

Course 2830—Three days—Instructor-led
Published: September 16, 2004

Introduction

Elements of this syllabus are subject to change.

This three-day, instructor-led course provides you with the knowledge and skills to design a secure network infrastructure. Topics include assembling the design team, modeling threats, and analyzing security risks in order to meet business requirements for securing computers in a networked environment. The course encourages decision-making skills through an interactive tool that simulates real-life scenarios that the target audience may encounter. You are given the task of collecting the information and sorting through the details to resolve the given security requirement.

Audience

This course is intended for IT systems engineers and security specialists who are responsible for establishing security policies and procedures for an organization. Students should have one to three years of experience designing related business solutions.

At Course Completion

After completing this course, you will be able to:

- Plan a framework for network security.
- Identify threats to network security.
- Analyze security risks.
- Design security for physical resources.
- Design security for computers.
- Design security for accounts.
- Design security for authentication.
- Design security for data.
- Design security for data transmission.
- Design security for network perimeters.
- Design an incident response procedure.

In addition, this course contains three teachable appendices that cover:

- Designing an acceptable use policy.
- Designing policies for managing networks.
- Designing an operations framework for managing security.

Prerequisites

This course requires that students meet the following prerequisites:

- A strong familiarity with Microsoft Windows® 2000 core technologies, such as those covered in Microsoft Official Curriculum (MOC) [Course 2152: Implementing Microsoft Windows 2000 Professional and Server](#).
- A strong familiarity with Windows 2000 networking technologies and implementation, such as those covered in MOC [Course 2153: Implementing a Microsoft Windows 2000 Network Infrastructure](#).
- A strong familiarity with Windows 2000 directory services technologies and implementation, such as those covered in MOC [Course 2154: Implementing and Administering Microsoft Windows 2000 Directory Services](#).

Microsoft Certified Professional Exams

- [Exam 70-220: Designing Security for a Microsoft Windows 2000 Network](#)
- [Exam 70-298: Designing Security for a Microsoft Windows Server 2003 Network](#)

Course Materials

The student kit includes a comprehensive workbook and other necessary materials for this class.

Course Outline

Module 1: Introduction to Designing Security

This module describes the basic framework for designing network security and introduces key concepts used throughout the course. It also introduces an ongoing case study that is utilized in the labs.

Lessons

- Introduction to Designing Security for Microsoft Networks

- Contoso Pharmaceuticals: A Case Study

Module 2: Creating a Plan for Network Security

This module discusses the importance of security policies and procedures in a security design. It also explains how a security design team must include representation from various members of your organization. After completing this module, you will be able use a framework for designing security and create a security design team.

Lessons

- Introduction to Security Policies
- Defining a Process for Designing Network Security

- Creating a Security Design Team

Lab A: Planning a Security Framework

After completing this module, you will be able to:

- Describe common elements of security policies and procedures.
- Create a security design framework by using the Microsoft Solutions Framework (MSF) process model.
- Create a security design team.

Module 3: Identifying Threats to Network Security

This module explains how to identify likely threats to a network and explains attacker motivations. After completing this module, you will be able to explain common threats and predict threats by using a threat model.

Lessons

- Introduction to Security Threats
- Predicting Threats to Security

Lab A: Identifying Threats to Network Security

After completing this module, you will be able to:

- Explain common network vulnerabilities and how

attackers can exploit them.

- Predict threats to security by using the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) threat model.

Module 4: Analyzing Security Risks

This module explains how to determine what resources in an organization require protection and how to categorize them in order to assign an appropriate level of protection. After completing this module, you will be able to apply a framework for planning risk management.

Lessons

- Introduction to Risk Management
- Creating a Risk Management Plan

Lab A: Analyzing Security Threats

After completing this module, you will be able to:

- Explain the purpose and operation of risk management.
- Draft the elements of a risk management plan.

Module 5: Creating a Security Design for Physical Resources

This module describes threats and risks to physical resources in an organization, as well as how to secure facilities, computers, and hardware. After completing this module, you will be able to design security for physical resources.

Lessons

- Determining Threats and Analyzing Risks to Physical Resources
- Designing Security for Physical Resources

Lab A: Designing Security for Physical Resources

After completing this module, you will be able to:

- Determine threats and analyze risks to physical resources.
- Design security for physical resources.

Module 6: Creating a Security Design for Computers

This module explains how to determine threats and analyze risks to computers on your network. After completing this module, you will be able to design security for computers.

Lessons

- Determining Threats and Analyzing Risks to Computers
- Designing Security for Computers

Lab A: Designing Security for Computers

After completing this module, you will be able to:

- Determine threats and analyze risks to computers.
- Design security for computers.

Module 7: Creating a Security Design for Accounts

This module describes the threats and risks to accounts in an organization. After completing this module, you will be able to design security for accounts.

Lessons

- Determining Threats and Analyzing Risks to Accounts
- Designing Security for Accounts

Lab A: Designing Security for Accounts

After completing this module, you will be able to:

- Determine threats and analyze risks to accounts.
- Design security for accounts.

Module 8: Creating a Security Design for Authentication

This module describes threats and risks to authentication. After completing this module, you will be able to design security for authentication.

Lessons

- Determining Threats and Analyzing Risks to Authentication
- Designing Security for Authentication

Lab A: Designing Authentication Security

After completing this module, you will be able to:

- Determine threats and analyze risks to authentication.
- Design security for authentication.

Module 9: Creating a Security Design for Data

This module examines threats and risks to data. After completing this module, you will be able to design security for data.

Lessons

- Determining Threats and Analyzing Risks to Data
- Designing Security for Data

Lab A: Designing Security for Data

After completing this module, you will be able to:

- Determine threats and analyze risks to data.
- Design security for data.

Module 10: Creating a Security Design for Data Transmission

This module discusses threats and risks to data transmission. After completing this module, you will be able to design security for data transmission.

Lessons

- Determining Threats and Analyzing Risks to Data Transmission
- Designing Security for Data Transmission

Lab A: Designing Security for Data Transmission

After completing this module, you will be able to:

- Determine threats and analyze risks to data transmission.
- Design security for data transmission.

Module 11: Creating a Security Design for Network Perimeters

This module describes threats to the points where your network connects to other networks, such as the Internet. After completing this module, you will be able to design security for network perimeters.

Lessons

- Determining Threats and Analyzing Risks to Network Perimeters
- Designing Security for Network Perimeters

Lab A: Designing Security for Network Perimeters

After completing this module, you will be able to:

- Determine threats and analyze risks to network perimeters.
- Design security for network perimeters.

Module 12: Designing Responses to Security Incidents

This module provides information about auditing and creating procedures to direct how you respond to security incidents. After completing this module, you will be able to design an audit policy and an incident response procedure.

Lessons

- Introduction to Auditing and Incident Response
- Designing an Audit Policy
- Designing an Incident Response Procedure

Lab A: Designing an Incident Response Procedure

After completing this module, you will be able to:

- Explain the importance of auditing and incident response.
- Design an auditing policy.
- Design an incident response procedure.

Appendices

Appendix A: Designing an Acceptable Use Policy

This appendix provides information about creating policies for acceptable use of network resources by users.

Lessons

- Analyzing Risks That Users Introduce
- Designing Security for Computer Use

Appendix B: Designing Policies for Managing Networks

This appendix offers guidelines for ensuring that network administrators manage networks in a secure manner.

Lessons

- Analyzing Risks to Managing Networks
- Designing Security for Managing Networks

Appendix C: Designing an Operations Framework to Manage Security

This appendix explains how to create a framework to ensure security of a network as the network changes and as the security requirements of the organization change.

Lessons

- Analyzing Risks to Ongoing Network Operations
- Designing a Framework for Ongoing Network Operations