

Course 2810 — Instructor-led

Course Length: 4 days

At the end of this course, students will be able to:

- Explain common attacks against network assets, the associated threats and vulnerabilities, and what network security personnel do to secure assets.
- Explain how to use cryptography to help protect information and how to choose an appropriate encryption method for an organization.
- Implement security-enhanced computing baselines in an organization.
- Help protect information in an organization by using authentication and access control.
- Deploy and manage certificates.
- Help protect transmission of data by identifying threats to network devices and implementing security for common data transmission, remote access, and wireless network traffic.
- Help protect Web servers against common attacks and configure security for Web browsers.
- Help protect e-mail messages and instant messaging from common security threats.

- Identify common security threats and vulnerabilities to directory services and DNS, and then apply security methods to help protect them.
- Identify network perimeter threats and monitor perimeter security for a network.
- Identify types of security policies to manage operational security, and then use these policies to ensure compliance by users in an organization.
- Preserve business continuity by implementing a security-enhanced disaster recovery strategy, communicating risks to others, and performing secure backup and recovery.
- Identify, respond to, and assist in the formal investigation of security incidents.

Prerequisites:

Before attending this class, students must have:

- One year of experience managing Windows 2000 Server or have equivalent knowledge and skills, such as those described in MOC Course 2152: Implementing Microsoft Windows 2000 Professional and Server.

Course Outline

Module 1: Preparing to Secure Information

Lessons

- Explaining How Assets Are Attacked
- Explaining How Assets Are Secured

Lab A: Preparing to Secure Information

Module 2: Implementing Security-Enhanced Computing Baselines

Lessons

- Introduction to Trusted Computing Bases
- Establishing a Security Baseline
- Monitoring a Security Baseline
- Helping to Secure Computers Physically
- Maintaining a Security Baseline

Lab A: Maintaining Baseline Security

Module 3: Helping to Protect Information Using Authentication and Access Control

Lessons

- Introduction to Access Control
- Implementing an Authentication Strategy
- Implementing an Access Control Strategy

Lab A: Securing Accounts (MBSA)

Module 4: Using Cryptography to Help Protect Information

Lessons

- Introduction to Cryptography
- Using Symmetric Encryption
- Using Hash Functions
- Using Public Key Encryption

Lab A: Using Cryptography to Help Protect Information

Fundamentals of Network Security

Course 2810 — continued

Module 5: Using a PKI to Help Protect Information

Lessons

- Introduction to Certificates
- Introduction to Public Key Infrastructure
- Deploying and Managing Certificates

Lab A: Using Certificates

Module 6: Securing Internet Applications and Components

Lessons

- Helping to Protect Web Servers
- Configuring Security for Common Internet Protocols
- Configuring Security for Web Browsers
- Configuring Security for Databases

Lab A: Securing Web Servers

Lab B: Protecting Clients from Active Content

Module 7: Implementing Security for E-Mail and Instant Messaging

Lessons

- Securing E-Mail Servers
- Securing E-Mail Clients
- Securing Instant Messaging

Lab A: Securing Mail Servers

Module 8: Managing Security for Directory Services and DNS

Lessons

- Helping protect Directory Services Against Common Threats
- Helping Protect DNS Against Common Threats

Lab A: Managing Security for Directory Services and DNS

Module 9: Securing Data Transmission

Lessons

- Identifying Threats to Network Devices
- Implementing Security for Common Data Transmission

- Implementing Security for Remote Access
- Implementing Security for Wireless Network Traffic

Lab A: Securing Data Transmission

Lab B: Using IPSec to Secure Data Transmission

Module 10: Implementing and Monitoring Security for Network Perimeters

Lessons

- Introduction to Network Perimeters
- Implementing Security on Inbound and Outbound Network Traffic
- Monitoring Network Traffic

Lab A: Implementing and Monitoring Security for Network Perimeters

Module 11: Managing Operational Security

Lessons

- Establishing Security Policies and Procedures
- Educating Users about Security Policies
- Applying Security Policies to Operational Management
- Resolving Ethical Dilemmas When Helping to Protect Assets

Lab A: Managing Operational Security

Module 12: Preserving Business Continuity

Lessons

- Preparing to Recover from Disasters
- Communicating the Impact of Risks
- Performing a Security-Enhanced Backup and Recovery

Lab A: Preserving Business Continuity

Module 13: Responding to Security Incidents

Lessons

- Identifying Security Incidents
- Responding to Security Incidents
- Investigating Security Incidents

Lab A: Responding to Security Incidents