



Course Syllabus

Fundamentals of Network Security

This four-day instructor-led course provides students with the knowledge and skills to begin supporting network security within an organization. Students who complete this course will be able to identify security threats and vulnerabilities and assist with responding to and recovering from security incidents.

This course will cover security concepts that are prerequisites for attending other Microsoft Official Curriculum (MOC) courses for security specialists and help prepare the student for the CompTIA Security+ exam. Although the course focuses on Microsoft product- and technology-specific implementation of security concepts, many of these same concepts can be applied to other technologies.

Audience

This course is designed for administrators who are responsible for the day-to-day administration of Microsoft® Windows® 2000. Students should have general knowledge of networking concepts and one or more years of experience managing Windows 2000. Other IT professionals may also take this course on the path to becoming a security specialist.

At Course Completion

After completing 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 secure information and how to choose an appropriate encryption method for an organization.
- Implement secure computing baselines in an organization.
- Secure information in an organization by using authentication and access control.
- Deploy and manage certificates.
- Secure data transmission by identifying threats to network devices and implementing security for common data transmission, remote access, and wireless network traffic.
- Secure Web servers against common attacks and configure security for Web browsers.
- 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 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 secure 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.

Key Data

Course #: 2810

Number of Days: 4

Format: Instructor-Led

Certification Exams:

This course helps you prepare for the following exams:

- CompTIA Security+ exam

Certification Track: None

This course syllabus should be used to determine whether the course is appropriate for the students, based on their current skills and technical training needs.

Course content, prices, and availability are subject to change without notice.

For a referral to a Microsoft Certified Technical Education Center in your area, see the Microsoft Training and Certification Web site at <http://www.microsoft.com/traincert>. Call your local Microsoft Certified Technical Education Center for more information and to register for classes.

Prerequisites

Before attending this course, 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*.

Module 1: Preparing to Secure Information

Lessons
<ul style="list-style-type: none">▪ Explaining How Assets Are Attacked▪ Explaining How Assets Are Secured
Lab A: Preparing to Secure Information

Module 2: Implementing Secure Computing Baselines

Lessons
<ul style="list-style-type: none">▪ Introduction to Trusted Computing Bases▪ Establishing a Secure Baseline▪ Monitoring a Secure Baseline▪ Physically Securing Computers▪ Maintaining a Secure Baseline
Lab A: Maintaining Baseline Security

Module 3: Securing Information Using Authentication and Access Control

Lessons
<ul style="list-style-type: none">▪ Introduction to Access Control▪ Implementing an Authentication Strategy▪ Implementing an Access Control Strategy
Lab A: Securing Accounts (MBSA)

Module 4: Using Cryptography to Secure Information

Lessons
<ul style="list-style-type: none">▪ Introduction to Cryptography▪ Using Symmetric Encryption▪ Using Hash Functions▪ Using Public Key Encryption
Lab A: Using Cryptography to Secure Information

Module 5: Using a PKI to Secure Information

Lessons
<ul style="list-style-type: none">▪ Introduction to Certificates▪ Introduction to Public Key Infrastructure▪ Deploying and Managing Certificates
Lab A: Using Certificates

Module 6: Securing Internet Applications and Components

Lessons
<ul style="list-style-type: none">▪ Securing 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
<ul style="list-style-type: none">▪ 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
<ul style="list-style-type: none">▪ Securing Directory Services Against Common Threats▪ Securing DNS Against Common Threats
Lab A: Managing Security for Directory Services and DNS

Module 9: Securing Data Transmission

Lessons
<ul style="list-style-type: none">▪ 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
<ul style="list-style-type: none">▪ 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
<ul style="list-style-type: none">▪ Establishing Security Policies and Procedures▪ Educating Users about Security Policies▪ Applying Security Policies to Operational Management▪ Resolving Ethical Dilemmas When Securing Assets
Lab A: Managing Operational Security

Module 12: Preserving Business Continuity

Lessons
<ul style="list-style-type: none">▪ Preparing to Recover from Disasters▪ Communicating the Impact of Risks▪ Performing a Secure Backup and Recovery
Lab A: Preserving Business Continuity

Module 13: Responding to Security Incidents

Lessons
<ul style="list-style-type: none">▪ Identifying Security Incidents▪ Responding to Security Incidents▪ Investigating Security Incidents
Lab A: Responding to Security Incidents

© 2003 Microsoft Corporation. All rights reserved.

Some elements of this course syllabus are subject to change. This syllabus is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.