

Course Outline

Other Information	
MS2150	
Days	5
Starting Time	9:00
Finish Time	4:30
Lunch & refreshments are included with this course.	

Designing a Secure Microsoft Windows 2000 Network

Introduction

This provides students with the knowledge and skills necessary to design a security framework for small, medium, and enterprise networks using Microsoft® Windows® 2000 technologies. This course contains four units that describe security in specific areas of the network:

- Unit 1, *Providing Secure Access to Local Network Users*
- Unit 2, *Providing Secure Access to Remote Users and Remote Offices*
- Unit 3, *Providing Secure Access Between Private and Public Networks*
- Unit 4, *Providing Secure Access to Partners*

MCP Exam

This course will help the student prepare for the following Microsoft Certified Professional exam:

- To be determined

Pre-Requisites

This course requires that students meet the following prerequisites:

- Working knowledge of Windows 2000 Directory Services
- Completion of course 1560, Upgrading Support Skills from Microsoft Windows NT 4.0 to Microsoft Windows 2000

OR

- Completion of course 2154, Implementing and Administering Windows 2000 Directory Services

OR

- Equivalent knowledge

Course Outline

Day 1

Ø Module 1—Assessing Security Risks

- Identifying Risks to Data
- Identifying Risks to Services
- Identifying Potential Threats
- Introducing Common Security Standards
- Planning Network Security

Ø Module 2—Introducing Windows 2000 Security

- Introducing Security Features in Active Directory
- Authenticating User Accounts
- Securing Access to Resources
- Introducing Encryption Technologies



Learning Solutions



Ph: 1300 TO TRAIN
1300 86 87246

Course Outline (Continued)

- Encrypting Stored and Transmitted Data
- Introducing Public Key Infrastructure Technology

Unit 1—Providing Secure Access to Local Network Users

Ø Module 3—Planning Administrative Access

- Determining the Appropriate Administrative Model
- Designing Administrative Group Strategies
- Planning Local Administrative Access
- Planning Remote Administrative Access

Lab

- Planning Secure Administrative Access

Day 2

Ø Module 4—Planning User Accounts

- Designing Account Policies and Group Policy
- Planning Account Creation and Location
- Planning Delegation of Authority
- Auditing User Account Actions

Lab

- Planning a Security-based OU Structure

Ø Module 5—Securing Windows 2000–Based Computers

- Planning Physical Security for Windows 2000–based Computers
- Evaluating Security Requirements
- Designing Security Configuration Templates
- Evaluating Security Configuration
- Deploying Security Configuration Templates

Labs

- Analyzing a Security Template
- Designing Customized Security Templates

Ø Module 6—Securing File and Print Resources

- Examining Windows 2000 File System Security
- Protecting Resources Using DACLs
- Encrypting Data Using EFS
- Auditing Resource Access
- Securing Backup and Restore Procedures
- Protecting Data from Viruses

Labs

- Managing EFS Recovery Keys
- Planning Data Security

Course Outline (Continued)

Day 3

Ø Module 7—Securing Communication Channels

- Assessing Network Data Visibility Risks
- Designing Application-Layer Security
- Designing IP-Layer Security
- Deploying Network Traffic Encryption

Lab

- Planning Transmission Security

Ø Module 8—Providing Secure Access to Non-Microsoft Clients

- Providing Secure Network Access to UNIX Clients
- Providing Secure Network Access to NetWare Clients
- Providing Secure Access to Macintosh Clients
- Securing Network Services in a Heterogeneous Network
- Monitoring for Security Breaches

Lab

- Securing Telnet Transmissions

Unit 2—Providing Secure Access to Remote Users and Offices

Ø Module 9—Providing Secure Access to Remote Users

- Identifying the Risks of Providing Remote Access
- Designing Security for Dial-Up Connections
- Designing Security for VPN Connections
- Centralizing Remote Access Security Settings

Lab

- Using RADIUS Authentication

Day 4

Ø Module 10—Providing Secure Access to Remote Offices

- Defining Private and Public Networks
- Securing Connections Using Routers
- Securing VPN Connections Between Remote Offices
- Identifying Security Requirements

Labs

- Planning Secure Connections for Remote Offices

Unit 3—Providing Secure Access Between Private and Public Networks

Ø Module 11—Providing Secure Network Access to Internet Users

- Identifying Potential Risks from the Internet
- Using Firewalls to Protect Network Resources
- Using Screened Subnets to Protect Network Resources
- Securing Public Access to a Screened Subnet

Course Outline (Continued)

Lab

- Designing a Screened Subnet

Ø Module 12—Providing Secure Internet Access to Network Users

- Protecting Internal Network Resources
- Planning Internet Usage Policies
- Managing Internet Access Through Proxy Server Configuration
- Managing Internet Access Through Client-Side Configuration

Lab

- Securing the Internal Network When Accessing the Internet

Day 5

Unit 4—Providing Secure Access to Partners

Ø Module 13—Extending the Network to Partner Organizations

- Providing Access to Partner Organizations
- Securing Applications Used by Partners
- Securing Connections Used by Remote Partners
- Structuring Active Directory to Manage Partner Accounts
- Authenticating Partners from Trusted Domains

Lab

- Planning Partner Connectivity

Ø Module 14—Designing a Public Key Infrastructure

- Introducing a Public Key Infrastructure
- Using Certificates
- Examining the Certificate Life Cycle
- Choosing a Certification Authority
- Planning a Certification Authority Hierarchy
- Mapping Certificates to User Accounts
- Managing CA Maintenance Strategies

Lab

- Using Certificate-based Authentication

Ø Module 15—Developing a Security Plan

- Designing a Security Plan
- Defining Security Requirements
- Maintaining the Security Plan

Lab

- Developing a Security Plan