

CIT 266

Windows 2000 Network Security

Course Description

This course 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 is part of the Microsoft Certified Systems Engineer series.

Prerequisites: CIT 261; or consent of instructor.

Course Competencies

Upon completion of this course, the student can:

1. Identify the security risks associated with managing resource access and data flow on the network
2. Describe how key technologies within Windows 2000 are used to secure a network and its resources
3. Plan a Windows 2000 administrative structure so that permissions are granted only to appropriate users
4. Plan an Active Directory™ directory service structure that facilitates secure and verifiable user account creation and administration;
5. Define minimum security requirements for Windows 2000-based domain controllers, application servers, file and print servers, and workstations
6. Design a strategy for securing local storage of data and providing secure network access to file and print resources
7. Design end-to-end security for the transmission of data between hosts on the network
8. Design a strategy for securing access for non-Microsoft clients within a Windows 2000-based network
9. Design a strategy for securing local resources accessed by remote users using dial-in or Virtual Private Network (VPN) technologies
10. Design a strategy for securing local resources accessed by remote offices within a wide area network (WAN) environment
11. Protect private network resources from public network users
12. Design a strategy for authenticating trusted users over public networks
13. Design a strategy for securing data and application access for the private network when accessed by trusted partners
14. Plan for an e-commerce implementation between your organization and external business partners that facilitates business communication
15. Design a structured methodology for securing a Windows 2000 network

Course Outline

- I. Assessing Security Risks
 - A. What is a Risk?
 - B. What are Potential Threats to the Network?
 - C. Describing Common Security Standards

- D. Planning Enterprise Security
- II. Introducing the Windows 2000 Security Model
 - A. The role of Directory Services in the Security Framework
 - B. Identifying Authentication Methods Available Within Windows 2000 Networks
 - C. Controlling Access to Resources on Windows 2000 Networks
 - D. Introducing Encryption Technology
 - E. Encrypting Stored and Transmitted Data in Windows 2000 Networks
 - F. Introducing Public Key Infrastructure Technology
- III. Providing Secure Access to Local Network Users
 - A. Planning Administrative Access
 - B. Planning User Accounts
 - C. Securing Windows 2000 Based Computers
 - D. Securing File and Print Resources
- IV. Securing Communication Channels on the Local Network
 - A. Assessing Network Data Visibility Risks
 - B. Evaluating Network Authentication Methods
 - C. Protecting Network Data Transmission from Packet-Level Impersonation
 - D. Encrypting Network Data Transmissions with Internet Protocol Security IPSec
- V. Providing Secure Access to Non-Microsoft Clients
 - A. Providing Secure Access to IP-Based Clients
 - B. Providing Secure Access to NetWare Clients
 - C. Providing Secure Access to Macintosh Clients
- VI. Providing Secure Access to Remote Users and Offices
 - A. Providing Secure Access to Remote Users
 - B. Providing Secure Access to Remote Offices
- VII. Providing Secure Access Between Private and Public Networks
 - A. Maintaining Security When Allowing Public Access to Your Private Network
 - B. Maintaining Security When Accessing Public Networks From Your Network
- VIII. Providing Secure Access to Partners
 - A. Authenticating Trusted Partners
 - B. Providing Secure Resource Access to Trusted Partners
 - C. Providing Business to Business and E-Commerce Security
 - D. Developing a Security Plan