


| | | | |
|---|---|--|--|
| <h1 style="margin: 0;">LearnKey® Training</h1> | <h1 style="margin: 0;">Windows 2000 Network Security Design</h1> | | |
| <div style="text-align: center;">  </div> <h2 style="margin-top: 20px;">Windows 2000 Network Security Design</h2> <p>3 Sessions – 9 Hours of Interactive Training</p> <hr/> <p>LearnKey's Windows 2000 Network Security Design course will give you the essential knowledge and skills to design and manage security on a Windows 2000 network. LearnKey expert Michael Storm shows you the critical steps of evaluating, creating, and implementing security, as well as providing strategies to meet specific security needs. At the conclusion of this course you will understand the security risks to a network and how to design and implement appropriate solutions, as well as be prepared to pass exam #70-220.</p> <p>Also Available:</p> <ul style="list-style-type: none"> - Study Guide - Test Prep <hr/> <p>About The Author</p> <p>For the past 16 years, Michael Storm has managed the design, security and implementation of enterprise networks for Fortune 100 companies around the globe. As the founder of Brainstorm International, Inc., Storm specializes in InfoSec Security and Internetwork Solutions Architectures. He is currently the Director of Network Engineering and Security Officer for Interface Technical Training of Phoenix, AZ and creator of the 'Hard Hat' learning process, used by countless Cisco and Microsoft Professionals for achieving technical mastery. Storm holds many IT certifications, including the Cisco CCIE Security, CCNP/CCSP/CCDP, NSA/CNSS CISSP, MCSE and MCT.</p> | <p>Session 1</p> <p>Section A: Security Design Process</p> <ul style="list-style-type: none"> - Security Design Categories - Risks to Data & Services - Security Design Process - Analyzing Business Requirements - Designing Security Baseline <p>Section B: Securing Windows 2000 Systems</p> <ul style="list-style-type: none"> - Security Baseline - Physical Security Planning - Hardware Configuration Security - Securing Passwords & Templates - Evaluating Security - Verifying & Analyzing a Security Baseline - Automating Security Analysis - Deploying Security Configurations - Guidelines for GPO Deployment - Processing Order of Policies - Identifying Effective Policy <p>Section C: Authentication Strategy Design</p> <ul style="list-style-type: none"> - Kerberos & Certificate-based - NTLM, Clear Text & Digest - Secure Sockets Layer & Radius - Determining Correct Authentication Method <p>Section D: Unix Authentication Strategy</p> <ul style="list-style-type: none"> - Integration with Unix Systems - Designing Unix Integration - NFS Access - Securing TCP/IP Programs <p>Section E: Macintosh Authentication Strategy</p> <ul style="list-style-type: none"> - Integrating with Macintosh - Macintosh Authentication - Designing the Macintosh Integration <p>Section F: NetWare Authentication Strategy</p> <ul style="list-style-type: none"> - Integrating with NetWare - NetWare Authentication - NetWare Connectivity Risk & Solution | <p>Session 2</p> <p>Section A: File & Print Strategy</p> <ul style="list-style-type: none"> - File System Security - Using DACLS & DACL Inheritance - NTFS & Share Permissions - Combining Permissions - Print Resources <p>Section B: EFS & Auditing</p> <ul style="list-style-type: none"> - EFS Features & Protection - EFS Recovery & Options - Audit Resources - Classified Auditing <p>Section C: Administrative Model</p> <ul style="list-style-type: none"> - Assigning Access - Centralized, Decentralized & Hybrid - Roles & Tasks Defined - Security Management <p>Section D: Local & Remote Administrative Access</p> <ul style="list-style-type: none"> - Planning Local - Run as Service - Planning Remote & Encryption Options - Securing VPN - Design Decisions <p>Section E: Terminal Services Security</p> <ul style="list-style-type: none"> - Remote Administration & Encryption Choices - Preferred Configuration - Telnet Administration <p>Section F: Delegation of Authority & Account Planning</p> <ul style="list-style-type: none"> - Planning - Account Placement - Custom & Nesting Groups - Managing Administrators <p>Section G: Audit & Account Policies</p> <ul style="list-style-type: none"> - Audit Policy - Audit Strategy - Design Policies - Group Policy - Inheritance <p>Section H: Public Key Infrastructure</p> <ul style="list-style-type: none"> - Certificate Uses & Requirements - CA Hierarchy - Third-party & Commercial CA's - Private CA | <p>Session 3</p> <p>Section A: PKI Design</p> <ul style="list-style-type: none"> - CA Guidelines - Availability - CA Usage & Organizational Hierarchy - Location Hierarchy <p>Section B: Certificate Management</p> <ul style="list-style-type: none"> - Mapping Certificates - CA Maintenance Strategies - Hardware & Compromise Recovery - Minimize Risk <p>Section C: Network Services Security</p> <ul style="list-style-type: none"> - DNS, RIS & SNMP Security <p>Section D: Secure Communication Channels</p> <ul style="list-style-type: none"> - Designing Security - SMB Signing - Designing an IPSec Solution - Selecting an IPSec Mode & Security Policies - IPSec Negotiations Policies & Filters - Managing IPSec <p>Section E: Remote-to-Private Networks</p> <ul style="list-style-type: none"> - Security Design Risks & Solutions - Avoiding Security Weaknesses - RAS Policies & Benefits of VPN Connections - Securing VPN Access - Using Radius to Centralize RAS Security <p>Section F: Private-to-Private Networks</p> <ul style="list-style-type: none"> - Security Design Risks & Solutions - Router Security <p>Section G: Public-to-Private Networks</p> <ul style="list-style-type: none"> - The Internet - Solutions - Using Firewalls - Using Screened Subnets - Avoiding Vulnerabilities <p>Section H: Securing Access to Private Networks</p> <ul style="list-style-type: none"> - Access to a Screened Subnet - Traffic to an Http and FTP Server - Traffic to a DNS & Messaging Server - Traffic to an Application Server - PPTP & L2TP Traffic to a Tunnel Server - Traffic to a Terminal Services Server <p>Section I: Analyzing Business Requirements</p> <ul style="list-style-type: none"> - Analyzing Structure of IT Management - Analyzing Technical Requirements - Security Design Summary |