



## Windows Server 2003 Security Implementation 5 Sessions –

15 Hours of Interactive Training

The Windows Server 2003 Security Implementation course from LearnKey prepares you with the knowledge and skills needed to implement, manage, maintain, and troubleshoot security in a Windows Server 2003 network infrastructure. Expert instructor Tom Carpenter shows you how to plan and implement security policies, patch management, network communications security, authentication / authorization / access (AAA), and public key infrastructure. LearnKey prep courses for Microsoft certification exams meet or exceed all exam objectives. At the conclusion of the course, you will be prepared to pass the MCP exam 70-299, Implementing and Administering Security for a Microsoft Windows Server 2003 Network.

### About The Author

**Tom Carpenter** has delivered training programs to more than 27,000 IT professionals since 1997. He has developed and delivered courses on Windows NT, 2000, XP and Server 2003. With experience as a Fortune 1000 systems administrator and security officer, Carpenter brings a wealth of real world experience and knowledge to his courses. Tom is Microsoft certified and is one of the founding managers of the Certified Technology Services Professional certification.

### Session 1

#### Section A: Introduction

- Prerequisites
- Foundations
- Threats
- Tools
- Principles

#### Section B: Security Structures

- Overview
- Users
- Groups
- Organizational Units
- Domains
- Trees
- Forests
- Site Management

#### Section C: Authentication

- Identity
- Process
- Protocols
- Kerberos

#### Section D: Implementing Authentication

- Password Policy
- Account Lockout Policy
- Kerberos Policy
- LM Authentication Level

#### Section E: Web Authentication

- Process
- Anonymous Access
- Authenticated Access
- Delegated Authentication
- Implementing

#### Section F: Trust Relationship

- Managing
- Types
- Authentication Methods
- SID Filtering
- Creating

#### Section G: Group Hierarchies

- Understanding Groups
- Types & Scopes
- Local & Domain Level
- Global & Universal
- Relationships
- Group Permissions

#### Section H: Group Types

- Functional Levels
- Built-in Groups
- Tools for Managing
- Net Group Command
- Restrict Groups

### Session 2

#### Section A: Authorization

- ACLs
- Processes
- Rules
- Permissions

#### Section B: Managing ACLs

- Security Permissions
- Security Settings
- Verifying Permissions
- Group Permissions
- Explicit Denial

#### Section C: Permissions

- Registry
- Printers
- AD Objects
- Services

#### Section D: Security Templates

- Planning
- Adding
- Built-in
- Copy
- New
- Configuration Based

#### Section E: Role-Based Templates

- Domain Controllers
- Event Log
- Audit Policy
- File Servers
- System Services
- Web Servers

#### Section F: Deploying Templates

- Create OUs
- Move OUs
- Create GPOs
- Edit GPOs
- Import Settings

#### Section G: Troubleshooting Templates

- GPUPDATE
- Synchronize Time
- GPO Permissions
- Adv System Info
- Run RSoP
- Resultant Wizard
- Event Viewer

#### Section H: Policies & Troubleshooting

- System Policies
- Troubleshooting.POL
- Policy Editor

### Session 3

#### Section A: Client Security

- Planning
- Determine Needs
- Client Roles
- Group Policy Editor
- Registry Editing
- Network Places
- Display Settings

#### Section B: Restricting Software

- Determining Restrictions
- Restricting Users
- Restricting Documents
- Restricting Levels
- Additional Rules
- Creating Hash Rule

#### Section C: Distributing Software

- Steps
- Read Access
- Distributing in AD
- Deployment Methods
- Deployment Methods

#### Section D: Securing Servers

- Determining Roles
- DNS & DHCP Servers
- Domain Controllers
- Integrating DNS
- Disabling Root Hints
- Securing Registry
- Authorizing DHCP
- Securing Logs & SysKey

#### Section E: Securing Web Servers

- IIS
- Enabling Web Extensions
- Securing Web Access
- Securing Web Properties

#### Section F: Securing Exchange Servers

- Precautions
- Exchange Ports
- Securing SQL Servers
- SQL Server Authorization
- MSSQL Server Logging
- Securing IAS Servers

#### Section G: Security Setting Analysis

- MBSA Tool
- Generate MBSA Report
- View MBSA Report
- MBSACL Report
- View MBSACL Report
- Sec Config & Analysis Tool
- Compare Security Settings

# Windows Server 2003 Security Implementation

## *continued*

### **Session 4**

#### Section A: PKI

- Essentials
- Terminology
- Hierarchies
- Certificate Needs

#### Section B: Installing Certificate Services

- Steps for Installation
- Configuring Installation
- Configuring Properties

#### Section C: Certification Templates

- Using Templates
- Default User Templates
- Default Computer Templates
- Default Service Templates
- Managing Templates
- Configuring Templates
- Creating New Certificate
- Requesting New Certificate

#### Section D: Managing Certificates

- Deploying & Revoking
- CRLs
- Viewing Certificates
- Enrolling in Certificates
- Requesting Certificates
- Requesting in IE
- Revoking Certificates

#### Section E: Backup & Restoration

- Configuring
- Exporting Keys
- Backing Up CA
- Backing Up System State

#### Section F: Wireless Security

- Overview
- Networking Threats
- Standards
- Authentication
- Encryption
- Best Practices
- Creating Network Policies
- Configuring Settings

### **Session 5**

#### Section A: Managing Updates & Patches

- Considerations
- Service Packs & Updates
- Chaining Updates
- Testing Procedures
- Updating Methods
- Tiered SUS Architecture
- Installing Updates
- Configuring Updates

#### Section B: Understanding IPSec

- Foundations
- Architecture
- Security Associations
- Policies
- Planning Configuring
- Troubleshooting

#### Section C: Managing IPSec

- Viewing Network Traffic
- Analyzing Network Traffic
- Creating New Filter
- Creating New Policies
- Implementing Policies
- Enabling Client

#### Section D: Managing SSL

- Deploying SSL
- SSL Ports
- Configuring Prerequisites
- Implementing SSL
- Enabling Certificates

#### Section E: Securing RRAS

- Fundamentals
- VPN Protocols
- Starting RRAS
- Configuring RRAS