

The Windows Server 2003 Security Design course prepares you with the knowledge and skills needed to analyze business requirements for a secure network infrastructure and design a security solution that meets those requirements. Expert instructor Tom Carpenter demonstrates how to create conceptual, logical, and physical designs for network infrastructure security. 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 70-298, Designing Security for a Microsoft Windows Server 2003 Network.

Session 1

Section A: Security Foundation

- Introduction
- Security
- Privacy
- Reliability
- Prerequisites

Section B: Security Policies

- Policies vs. Procedures
- Creating Policies
- Policy Procedures
- Tips
- End-user Impact

Section C: Data Security

- Data Classification
- Data Flow
- Data Vulnerability
- Data Categories
- Category Options

Section D: Business Requirement

- Cost Analysis
- Legal Issues
- Interoperability
- Maintainability
- Scalability

Section E: Technical Constraints

- Infrastructure
- Technology
- Interoperability
- Analyzing

Section F: Design Principles

- Defense
- Access/Access Points
- Authentication
- Implementation
- CIA

Section G: Security Framework

- 5 Factors
- Design Team
- Threat Prediction
- Threat Modeling
- Threat Detection
- Threat Response

Section H: Risk Management

- Business Impact Analysis
- Business Continuity Planning
- Agents of Threat
- Risk Ratings
- Management Options

Session 2

Section A: Network Management Procedures

- Secure Administration
- Privileged Groups
- Secure Systems
- Tasks & Duties
- Secure Practices
- Securing Tools
- Locking Tools
- Remote Administration

Section B: Secure Maintenance

- Software Deployment
- Patch Detection
- EMS

Section C: Software Updates

- SUS
- Server-Side
- Client-Side
- Requirements
- Administration

Section D: Authentication

- Risks
- Server Methods
- Kerberos
- Strategy
- Certificates

Section E: File & Folder Access

- Permissions Management
- Permission Inheritance
- Effective Permissions
- Auditing
- Group Management

Section F: File & Folder Security

- Encrypting
- Backup & Recovery
- Registry Security
- Printer Security

Section G: Remote Access

- Security Issues
- Accessing Resource
- Policies
- RADIUS
- IAS
- NAQC

Section H: VPN Security

- VPN Traffic
- Tunneling Protocol
- Authentication

Session 3

Section A: Network Infrastructure

- Domain/Forest Structures
- Transitive Trust
- Demand-dial Routing
- Firewall Configuration
- Secure Transmission
- IPSec
- IP Filtering

- IPsec Policy
- Section B: Securing DNS
 - Understanding DNS
 - Common Attacks
 - Methods
 - DNS Options
- Section C: Perimeter Security
 - Segmented Networks
 - Internal Segmentation
 - Extranets
 - Cross-Certification
- Section D: PKI Overview
 - PKI Services
 - PKI Terms
 - PKI Processes
 - Internal vs. External
- Section E: PKI Planning
 - Determine Needs
 - Certificate Usage
 - Hierarchy
 - Distribution
 - Management
 - CA Security

Session 4

- Section A: Server Baselines
 - Baseline Options
 - Recommendations
 - Security Templates
 - Create Policies
 - Using Templates
- Section B: AD Security
 - AD Delegation
 - Delegation Scenario
 - Access Control
- Section C: Client Security
 - Client Threats
 - Hardening Clients
 - Restrictions
 - System Restrictions
- Section D: Wireless Essentials
 - Basic Infrastructure
 - Public Networks
 - Private Networks
- Section E: Wireless Security
 - Wireless Threats
 - Wireless Standards
 - Authentication
 - Encryption
 - Access Point
 - Best Practices