

Course Outline

2823 – Implementing and Administering Security in a Microsoft Windows Server 2003 Network



Duration: 5 days (30 hours)

Learning Objectives:

- Plan and configure an authorization and authentication strategy
- Install, configure, and manage certification authorities
- Configure, deploy, and manage certificates
- Plan, implement, and troubleshoot smart card certificates
- Plan, implement, and troubleshoot Encrypting File System (EFS)
- Plan, configure, and deploy a secure member server baseline
- Plan, configure, and implement secure baselines for server roles
- Plan, configure, implement, and deploy client computer baselines
- Plan and implement software updates
- Plan, deploy, and troubleshoot data transmission security
- Plan and implement security for wireless networks
- Plan and implement perimeter security with Internet Security and Acceleration (ISA) Server 2004
- Secure remote access

Target Audience:

The course is for a system administrator or system engineer who has the foundation implementation skills and knowledge for the deployment of secure Microsoft Windows Server 2003 based solutions. This course is not intended to provide design skills, but will cover planning skills at a level sufficient to enable decision making for the implementation process

Prerequisites:

- Completed MOC 2810 or equivalent knowledge
- Experience implementing a Windows 2000 or Windows Server 2003 Active Directory environment. Experience with organizational resources such as Web, FTP and Exchange servers, (not expected to have detailed knowledge) shared resources and network services such as DHCP, DNS and WINS also helpful

Topics Covered:

- Planning and configuring an authentication and authorization strategy
 - Components of an Authentication Model
 - Planning and Implementing an Authentication Strategy
 - Groups and Basic Group Strategy in Windows Server 2003
 - Creating Trusts in Windows Server 2003
 - Planning, Implementing, and Maintaining an Authorization Strategy Using Groups
 - Planning and configuring an authentication and authorization strategy

- Planning and implementing a resource authorization strategy
- Planning and implementing a cross-forest authentication strategy
- Planning and implementing an authentication policy
- Installing, configuring, and managing certification authorities
 - Overview of a PKI
 - Introduction to Certification Authorities
 - Installing a Certification Authority
 - Managing a Certification Authority
 - Backing Up and Restoring a Certification Authority
 - Installing and configuring a certification authority
 - Installing an Enterprise Subordinate Certification Authority
 - Backing up a Certification Authority
- Configuring, deploying, and managing certificates
 - Overview of Digital Certificates
 - Deploying and Revoking User and Computer Certificates
 - Configuring Certificate Templates
 - Managing Certificates
 - Deploying and managing certificates
 - Configuring Multipurpose Certificate Templates
 - Configuring Certificate Autoenrollment
 - Updating a Certificate Template
 - Implementing a Key Archiving Strategy
- Planning, implementing, and troubleshooting Smart Card Certificates
 - Introduction to Multifactor Authentication
 - Planning and Implementing a Smart Card Infrastructure
 - Managing and Troubleshooting a Smart Card Infrastructure
 - Implementing Smart Cards
 - Configuring a Smart Card Enrollment Station
 - Simulation: Enrolling Users for Smart Cards
- Planning, implementing, and troubleshooting Encrypting file system
 - Introduction to EFS
 - Implementing EFS in a Standalone Microsoft Windows XP Environment
 - Planning and Implementing EFS in a Domain Environment
 - Implementing EFS File Sharing
 - Troubleshooting EFS
 - Planning, implementing, and troubleshooting Encrypting file system
 - Implementing certificates to support EFS
 - Configuring group policy to support EFS
- Planning, configuring, and deploying a secure member server baseline
 - Overview of a Member Server Baseline
 - Planning a Secure Member Server Baseline
 - Configuring Additional Security Settings
 - Deploying Security Templates
 - Securing Servers by Using the Security Configuration Wizard
 - Planning a Member Server Baseline

- Planning a secure member server baseline
- Planning, configuring, and implementing secure baselines for server roles
 - Planning and Configuring a Secure Baseline for Domain Controllers
 - Planning and Configuring a Secure Baseline for DNS Servers
 - Planning and Configuring a Secure Baseline for Infrastructure Servers
 - Planning a Secure Baseline for File and Print Servers
 - Planning and Configuring a Secure Baseline for IIS Servers
- Planning, configuring, implementing, and deploying a secure client computer baseline
 - Planning and Implementing a Secure Client Computer Baseline
 - Securing Applications on Client Computers
 - Planning and Implementing a Software Restriction Policy
 - Implementing Security for Mobile Clients
 - Planning, implementing, configuring, and deploying a secure client computer baseline
- Planning and implementing Software updates
 - Introduction to Software Update Management
 - Implementing Microsoft Baseline Security Analyzer
 - Installing Windows Server Update Services
 - Managing a WSUS Infrastructure
 - Planning and implementing software updates
 - Configure MBSA integration with WSUS server
- Planning, Deploying, and Troubleshooting Data Transmission Security
 - Secure Data Transmission Methods
 - Introducing IPSec
 - Planning and Implementing Data Transmission Security Using IPSec
 - Troubleshooting IPSec Communications
 - Implementing and troubleshooting data transmission security
 - Planning IPSec Security
 - Implementing IPSec Security
- Planning and Implementing Security for Wireless Networks
 - Introduction to Securing Wireless Networks
 - Implementing 802.1x Authentication
 - Planning a Secure WLAN Strategy
 - Implementing a Secure WLAN
 - Troubleshooting Wireless Networks
 - Planning and Implementing Security for Wireless Networks
 - Configuring Active Directory for Wireless Networks
 - Configuring Certificate Templates and Certificate Autoenrollment
 - Configuring Remote Access Policies for Wireless Devices
 - Configuring Group Policy for Wireless Networks
- Planning and Implementing Perimeter Security with Internet Security and acceleration Server 2004
 - Introduction to Internet Security and Acceleration Server 2004
 - Installing and Managing ISA Server 2004
 - Securing a Perimeter Network by Using ISA Server 2004
 - Publishing Servers on a Perimeter Network
 - Planning a Perimeter Network

- Implementing a Perimeter Network
- Securing an ISA Server 2000 Computer
- Securing Remote Access
 - Introduction to Remote Access Technologies and Vulnerabilities
 - Planning a Remote Access Strategy
 - Deploying Network Access Quarantine Control Components
 - Implementing a Secure VPN Solution
 - Configuring a VPN Connection
 - Configuring the VPN Server for Remote Access Quarantine
 - Configuring a Connection Manager Service Profile