

# Implementing Security in Win2K3

page 1

**Meet the expert:** Rafiq Wayani has extensive experience including more than 20 years in IT as Systems Architect, Software Engineer, DBA, and Project Manager. Wayani has instructed in a variety of technical areas, has designed and implemented network and information systems, and is certified across a wide range of platforms and systems including Microsoft Solutions Developer, Systems Engineer, Application Developer, Database Administrator, Trainer; Novell Netware Administrator and Engineer; Master Certified Netware Engineer; and A Certified.

**Runtime:** 08:15:16

**Course description:** Implementing and Administering Security in a Windows Server 2003 Network course will give you the knowledge and skills necessary to prepare to pass Microsoft exam 70-299. This course serves as an elective course for individuals pursuing the MCSA or MCSE on Windows Server 2003 certification.

## Course outline:

### Security Design

- Introduction
- Designing Security Overview
- Reasons to Design Security
- Defense in Depth
- Least Privilege
- Minimize Attack Surface
- Design Security
- Install Active Directory Demo
- Add Client to Domain Demo
- Install Adminpak.msi Demo
- Install gpmmc.msi Demo
- Summary

### More on Security Design

- Introduction
- Security Implementation
- Network Security Overview
- Setup MMC with Tools
- Group Policy Management
- Enforce a Policy on Client
- Network Security Plan
- Standard Policy
- Suggested Policy
- Suggested Policy Demo
- Update Group Policy
- RunOnce Registry Key
- Group Policy Precedence
- Security Filtering Group Policy
- Summary

### Policies and Procedures

- Introduction
- Procedures Overview

- Reasons Why Policies Fail
- Creating Policies/Procedures
- Create New Policies Demo
- Link a GPO to an OU
- Allow Term. Serv./Local Login
- Use gpupdate /force
- Domain vs. Local S.P.
- Rem. Desktop Access Demo
- Summary

### Microsoft Solutions Framework

- Introduction
- MSF Overview
- Planning Phase
- Building Phase
- Managing Phase
- Building a Team
- Building the Extended Team
- Setting up a Forest Trust Demo
- Raise Domain Functional Level
- Raise Forest Functional Level
- Check DNS Forwarders
- Run the New Trust Wizard
- Create Other Side of Trust
- Confirm the Trusts
- Test the Trust Relationship
- Summary

### Plan/Configure Security

- Introduction
- Security Components
- Authentication
- Authorization
- Least Privilege

- Authentication Protocols
- Password Storage
- Auth. w/Group Policy Demo
- G.P. Results Wizard Demo
- Summary

### Plan/Config. Password Policy

- Introduction
- Passwords Overview
- How to Lockout Accounts
- Restrict Computer Access
- View/Set Password Policy
- View/Set Acct. Lockout Policy
- Supplemental Authentication
- Group Types/Scopes
- Restricted Group Policy
- View/Set Delegation
- View/Set Restricted G.P.
- Ways to Access Group Policies
- Set Lockout Tasks
- Set Audit Tasks
- Access Advanced Features
- Summary

### Encrypted File System (EFS)

- Introduction
- Encrypted File System
- Common Issues
- Implementation
- Data Recovery Agent (DRA)
- Using EFS in Explorer
- Using certmgr.msc
- Create/Implement DRA
- Using cipher.exe

- Test DRA
- Important EFS Pitfall
- Summary

### Security Templates / Tools

- Introduction
- Apply Latest Updates Demo
- Configure Automatic Updates
- Sec. Config. and Analysis Tool
- Create a Security Template
- Resultant Set of Policy (RSOP)
- MS Baseline Security Analyzer
- Rename Admin/Guest Account
- Security Configuration Wizard
- Summary

### Securing Servers

- Introduction
- Threats to Domain Controllers
- Implementing Security Policies
- Securing Active Directory (AD)
- Determine if Computer is a DC
- Moving Active Directory Demo
- Use NTDSUtil
- Check New AD Location
- Summary

### Windows Update Services

- Introduction
- Software Update Services
- Requirements for SUS
- Install SUS
- Configure SUS
- Using SSL with SUS
- Backup SUS
- Restore SUS

(Continued on page 2)

# Implementing Security in Win2K3

page 2

- Best Practices
- Summary

## IP Security

- Introduction
- IPSec Overview
- Securing Network Environment
- Create IPSec Policy on Client
- Create IPSec Policy on Server
- Manage Filter Lists/Actions
- Default IPSec Policies
- netsh tool
- IP Security Monitor
- Main Mode/Quick Mode
- Inet Conn. Sharing / Firewall
- Prohibit ICS/Firewall
- Routing and Remote Access
- Config. Routing/Rmt. Access
- Routing/Rmt. Enhancements
- Common IPSec Config Errors
- Summary

## Certificates

- Introduction
- Digital Certificates
- Contents of a Certificate
- Certificate Enrollment Methods
- Revoking Certificates
- Certificate Templates
- Certificate Keys
- Install Certificate Services
- Request a User Certificate
- Install a Certificate
- View the Certificate
- Revoke a Certificate
- Publish Revoked Certificates
- View Revoked Certificate List
- View Certificate Templates
- Create New Cert. Template
- Export a Certificate
- Backup Certificate Authority
- Restore Certificate Authority
- Summary

## Secure Sockets Layer

- Introduction
- SSL Comm. Overview
- SSL Comm. Definition
- How SSL Works
- Private/Public Key Definition
- Private/Public Key Auth.
- Certificates Overview
- Symmetric Key
- Hash
- Public Key Infrastructure (PKI)

- Securing a Website Demo
- Summary

## Wireless

- Introduction
- Wireless Networks
- Benefits
- Security Threats
- Wireless Standards
- Wireless Security
- Wireless Network Policies
- View/Set Wireless Policies
- Setup Wireless on Client
- View Access Point Config.
- Summary

## Windows 2003 Security

- Introduction
- Securing Domain Controllers
- Configure Auditing
- Rename Admin/Guest Account
- Configure Event Log Settings
- Filter Event Logs
- Save a Log File
- Configure NTFS Security
- Configure Security Options
- Auditing Config. Guidelines
- DNS Overview
- DNS Security Options
- Protecting DNS Servers
- DNS: AD Integrated DNS
- DNS: Update Credentials
- DNS: Secure Zone Replication
- DNS: Prevent Auth. Access
- Securing DHCP Servers
- Summary

## Client Security

- Introduction
- Securing Windows Clients
- Administrative Templates
- View Administrative Templates
- Custom Admin Templates
- View Custom Template Details
- Remove an Admin Template
- Admin vs. Security Templates
- Software Restriction Policy
- SRP Demo
- How Apps. Identify Software
- Considerations with SRP
- Summary

## Network Access - Part 1

- Introduction
- Components
- Server
- Requirements

- Types of Clients
- Security
- Setup Remote Access
- Manage Users Permissions
- Config. Routing/Rmt. Access
- Connect through VPN
- Connect as a Client
- Failed Connect Attempt
- Summary

## Network Access - Part 2

- Introduction
- VPN Connection
- Connection Process
- Components
- Encryption Protocols
- Encryption Requirements
- Wireless
- Two Modes for Wireless
- Wireless Components
- Wireless Standards
- 802.1x Authentication
- Win XP Client Config Types
- Determine Auth. Methods
- Dial-In Permissions
- Other Permissions
- Remote Access Policy
- Specify Rmt. Access Policies
- Config. Rmt. Access Logging
- Specify Dial-In Perm./Prop.
- Raise Domain/Forest Levels
- Summary