

Control and Security of Windows HANDS-ON

Course Duration: 1 Day or 2 Day
CPE Hours: 8 Hours or 16 Hours
Level: Intermediate/Group-Live
Prerequisites: None
Advanced Preparation: None

This seminar provides the participants with an overview of the technology, an understanding of the critical components and the risks associated with the Windows Server operating system. The Canaudit Risk/Control Tables and Windows Server Audit Guide are incorporated into this class to facilitate the participants' first Windows Server Audit. Participants are required to have a network-enabled Win2K/XP/Vista laptop with administrative rights to both the operating system and anti-virus software (to create a directory exempt from anti-virus scanning), an office suite with word processing and spreadsheet capabilities (i.e. MS Word and Excel), and a CD-ROM drive.

Who Should Attend:

This seminar is intended for IT auditors and security staff who desire an understanding of the Windows Server environment and the controls required to secure this environment.

Seminar Outline:

I. Overview of Windows Server

- New features
- Active Directory
- Additional security features
- The need for obsolesce

II. Windows Architecture

- The Executive mode
- The User mode
- The registry
- PDC emulation in mixed mode
- Mixed mode security
- Risk/Control Tables

III. Active Directory

- Major improvements
- Domains
- Domain trees and forests
- Domain trusts
- Physical structure
- Logical structure
- Organizational units
- Object access permissions
- Delegating administrative tasks
- Risk/Control Tables

IV. User and Group Management

- Administrator accounts
- Backup Operator accounts

- Local user accounts
- Domain user accounts
- User profiles
- Account security
- Group management
- Domain local groups
- Global groups
- Universal Groups
- Group Policy Management
- Risk/Control Tables

V. Hardening the Server

- Trustworthy Computing Initiative
- Restricted access
- Software Update Services
- Malware prevention techniques
- Vulnerability assessment and remediation
- Risk/Control Tables

VI. File Security

- NTFS Permissions
- Permission in heritage
- Folder ownership
- Shared access
- Distributed File System Sharing
- Risk/Control Tables

VII. Terminal Services and IIS

- Caution, you are entering a danger zone

- Configuring Terminal Services
- Terminal Services Administration requirements
- Use of Internet Information Services
- Security features
- IIS Components
- Risk/Control Tables

VIII. Using Kerberos Authentication

- Kerberos basics
- Policies
- Cross-Forest Authentication
- Public Keys
- Risk/Control Tables

IX. Securing Remote Connections

- VPN's in the MS server environment
- Encryption
- Tunneling
- Using Radius
- IPsec
- Risk/Control Tables

X. The Audit Guide

- The Canaudit Windows Server Audit Guide