

Control and Security of Windows and SQL Server HANDS-ON

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

This hands-on workshop will teach participants the skills needed to perform a vulnerability assessment and penetration test of the Windows and SQL Server environments. Over the course of the two days, participants will complete a series of simulations and exercises designed to build the knowledge to safely and sanely use freely available tools. These tools identify critical security issues in the enterprise-wide network. To assist in the transfer of skills, the workshop instructors are available post-seminar to provide assistance. 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 technically-able IT Auditors and security staff who desire a hands-on course in how to perform a complete Windows or SQL Server vulnerability assessment from initial scanning to reporting.

Seminar Outline:

I Introduction

- The Canaudit methodology
- Skill sets required
- Tools and techniques
- Anticipating the hurdles
- Preparing project plan
- Schedule testing
- Communicating project to IT group
- Getting started

II Mapping the Network

- Scanning the network
- Categorizing devices (Windows, UNIX, Linux, AS/400, Mainframe, databases)
- Building the master spreadsheet
- Risk assessment by machine category
- Identifying vulnerable systems
- Safe and sane testing techniques

III Assessing the Windows Environment

- The Windows environment
- The Canaudit Windows pen test methodology
- Domain and workstation identification
- Testing for critical flaws
- Demonstration of common Windows vulnerabilities
- Leveraging flaws to enhance access
- Accessing critical applications
- Work papers reporting and remediation plans
- Hands-on Windows practice audits

IV Assessing SQL Server Instances

- SQL Server in the network environment
- Auditing SQL Server service accounts
- Users and authentication controls
- Auditing and logging at a database level
- Configuring the database
- Securing dangerous procedures and functions
- Table, procedure and function permissions
- Securing data through encryption
- Honey pots, IDS, IPS
- Password auditing
- The SQL injection attack vector
- Work papers reporting and remediation plans
- Hands-on SQL Server practice audits