

Course 579

Windows 2008, 2008 R2 and Windows 7 Security Foundations (5 days)

Course Description...

In this advanced hands-on course, students will learn to enhance security on Windows 2008, Windows 2008 Release 2 (R2) and Windows 7. These products represent the current operating systems from Microsoft and are designed to provide secure Server and Desktop platforms. Starting with out-of-the-box installations, students will experience different types of vulnerabilities and the technologies necessary to minimize system exposure.

Topics such as Cryptography, Digital Certificates, Public Key Infrastructure (PKI), Encryption File System (EFS), Service and Application Security, Spyware/Malware, Network Monitoring, IP Security (IPSec), and Virtualization will be discussed and practiced.

Who should attend...

This will benefit System Administrators, Network Administrators, Developers, and Managers who need to understand how security affects the Windows platforms on corporate networks.

Suggested Prerequisites...

- Experience with Windows Desktop and/or Server Operating System Management
- NOTE: It is recommended student have a foundation course in Windows 2008, Windows 2008 R2 or Windows 7 before attending this course

Course Outline...

Chapter 1: Security Fundamentals

Windows 2008, 2008 R2 and Windows 7 Security Overview

Areas of Security: OS, Services, Local & Network Applications, Networking Protocols

Workshop: How good is security out-of-the-box? Testing with MBSA, Nessus & NMAP

Authentication: NTLM & Kerberos

Cryptography Primer: Symmetric, ASymmetric, & Hashing Algorithms

Digital Certificates & Public Key Infrastructure

Workshop: Digital Signing & Encryption Workshop



Chapter 2: Operating System Security

Operating System Updates: Hotfixes, Service Packs, Optional Updates

System Services: Mapping to Executables/Processes/Port Usage

Workshop: Removing non-essential services

System & Application Logs

Application startup

Registry Usage and Security

Workshop: Detecting and Removing unauthorized programs

Malware/Spyware

Microsoft Windows Anti-spyware add-on

Workshop: Install and configure Microsoft Windows Anti-spyware

Chapter 3: Application & Browser Security

Monitoring Application Access

Workshop: Viewing all files used by applications

Web Browser (Internet Explorer) Security

Active Components presented through Web Browsers

Workshop: Defining and Controlling Web Browser configuration

Virtualization: Good or Bad for Security

Securing Virtual Servers and Core-only installations of Windows Server

Workshop: Analysis of Virtual Server Security and Core Installations

Chapter 4: Network Security

Monitoring your network

Common Port Usage & Application identification

Workshop: Network Monitoring with Ethereal

Windows Firewall

Workshop: Configuring the Windows Firewall

Port filtering on the TCP/IP Stack

Enabling IP Security (IPSec)

Workshop: Configuring IPSec for enterprise usage

Enterprise Storage: iSCSI and network security

Chapter 5: File & Folder Security

Windows File & Folder Permissions

Examining Inheritance of Access Control Lists (ACLs)

Utilizing DACLs & SACLs effectively

Workshop: Securing the File System

BitLocker and BitLocker to Go configuration

Enterprise configuration of BitLocker for data recovery

Workshop: Configure BitLocker for Enterprise Usage & Recovery

Chapter 6: Active Directory Security

Windows Active Directory Security

Workshop: Raising the default security of the Active Directory

Securing AD Enabled Applications

Workshop: Secure AD Enabled DNS Zones & DHCP Registration



Chapter 7: Putting it all together

Review of key concepts

Workshop: Security Assessment: Repair a troubled infrastructure

***Attendees will be presented with a Windows 2008 Server and a Windows 7*

Workstation with multiple security issues. Students must successfully repair the problems and minimize security vulnerabilities.

Additional/Custom Topics are available - please contact your ROI representative to discuss course tailoring!!!