Windows Security

Course Overview

This is 5 day practical windows security training course, gain an understanding of the knowledge and skills needed to configure and manage the security of Windows systems and networks, including: Group Policy, Active Directory, DNS, Internet Information Server (IIS), IPSec , RADIUS, VPNs, BitLocker/EFS, and Certificate Services.

Target Audience

- Individuals responsible for installing, configuring, and securing Microsoft systems and Active Directory networks
- System and Network Administrators who are looking for guidance on specific tangible steps they can take to make their networks, servers, and client nodes more secure.

Course Pre-requisites

- Basic Windows skills and fundamental understanding of computer and networking concepts are required.
- Candidates should be familiar with Windows XP/Server 2003 through Windows 7/Server 2008 R2.

Course Details

(DAY 1)

- Introduction :
  - Understanding Risk
  - Exploring Security Triad
  - Defense in depth security strategy
  - Principle of least privilege
  - Server Hardening
- Securing Active Directory and DNS :
  - Read - Only Domain Controllers (RODC)

info@itsecurityct.com
www.itsecurityct.com

- Securing Domain Controllers
- SYSKEY.EXE
- Disaster Planning and Recovery
- Encrypting Replication Traffic
- Property - Level Permissions (DACLs)
- Audit Settings (SACLs)
- Delegation of Authority
- Organizational Unit Design
- Custom MMC Consoles
- The "Empty Root" Domain Model
- Best Practices for Forest Design
- DNS SRV Records
- Unix BIND Integration
- Secure Dynamic Updates
- Best Practices for Securing DNS

(DAY 2)

- Group Policy :
  - The Group Policy Management Console (GPMC)
  - Security Templates
  - Security Configuration and Analysis MMC Snap-In
  - SECEDIT.EXE
  - Group Policy Objects (GPOs)
  - GPO Links to Domains, OUs and Sites
  - Order of Precedence Processing: LSDOU
  - WMI Filtering
  - Custom ADM/ADMX Templates
  - MSI Deployment through Group Policy
  - Pushing Out Scripts
  - Software Restriction Policies
  - Managing Internet Explorer Settings
  - Replacing the Desktop Interface
  - Micro - Managing Users' Applications

(DAY 3)

- PKI, EFS and BitLocker:
  - Why Must I Have A PKI?
  - Examples: Smart Cards, VPNs, Wireless, SSL, S/MIME, etc.
  - How To Install The Windows PKI
  - Root vs. Subordinate Certification Authorities
  - Should You Be Your Own Root CA?
  - Controlling Certificate Enrollment
  - How To Manage Your PKI
  - Group Policy Deployment of Certificates
  - How To Revoke Certificates
  - Automatic Private Key Backup
  - Delegation of Authority
  - Deploying Smart Cards
  - Smart Card Enrollment Station
  - Best Practices for Private Keys
  - Encrypting File System
  - EFS Insecurity Myths
  - BitLocker Drive Encryption
  - TPM and USB BitLocker Options
  - BitLocker Emergency Recovery
  - MANAGE - BDE.WSF
  - Best Practices for EFS and BitLocker

(DAY 4)

- IPSec, Windows Firewall, NPS, VPNs and Wireless:
  - Secure Socket Tunneling Protocol (SSTP)
  - Isn't IPSec Just For VPNs? No!
  - IPSec Domain Isolation
  - How to Create IPSec Policies
  - Group Policy Management of IPSec
  - NETSH.EXE
  - Windows Firewall with Advanced Security
  - Configuring RADIUS Policies (NPS)
  - EAP vs. PEAP
  - PEAP - MS
  - CHAPv2
  - Smart Cards for VPN
  - IPSec + L2TP = RRAS VPNs
  - L2TP vs. PPTPv2
  - Host-to-Router VPN Configuration Steps
  - Router-to-Router VPN Configuration Steps
  - VPN Best Practices
  - Securing Wireless Networks
  - Wi-Fi Protected Access (WPA)
  - Smart Cards for Wireless
  - Best Practices for Wireless

info@itsecurityct.com
www.itsecurityct.com

(DAY 5)

- Securing IIS :
  - FTP Over SSL (FTPS)
  - IIS Server Hardening
  - Security Template for IIS
  - Patch Management
  - Removing Dangerous Services
  - Securing WebDAV
  - Managing Bindings
  - Hardening TCP/IP
  - IPSec for IIS Servers
  - Authentication Options
  - Kerberos and NTLM for Web Applications
  - Smart Cards for Web Applications
  - Minimal HTTP Permissions
  - Minimal NTFS Permissions
  - Proper NTFS Auditing
  - Running Scripts and Binaries on IIS
  - Web-Based Applications
  - Worker Process Isolation
  - HTTP.SYS Filtering
  - Securing XML Config Files
  - Securing Logs Hands-Free
  - Finding Hacking Signatures In Logs

info@itsecurityct.com
www.itsecurityct.com

- PowerShell Scripting:
    - What is PowerShell?
    - CmdLets
    - Running Scripts
    - Namespace Providers
    - Piping .NET Objects
    - Parameter Binding
    - Regular Expressions
    - Functions and Filters
    - The .NET Class Library
    - Using Properties and Methods at the Command Line
    - Security and Execution Policy
    - Managing the Event Logs
    - Accessing COM Objects: WMI, ADSI, ADO, etc.

Knowledge gain:

The following ten domains are covered in this course.

- Fundamentals of implementing file servers in Server 2008.
- Knowing how to create partitions, set up folder structure, how to manage and share folders.
- Securing Windows Server 2008/2003 network
- Knowing how to set NTFS Permissions and knowing how to secure files and folders for the Users and Groups
- Configuring and using Security Auditing is going to allow you to keep track of specific security events
- Setting up a Security Template on an individual system is a great way to configure your security settings
- Knowing how to install and configure this service will save the administrator time and in the long run, money

info@itsecurityct.com
www.itsecurityct.com

- Knowing how to implement PKI is necessary for the administrator that wants a root of trust for technologies that use digital certificates
- Knowing how to use EFS and the various enhancements of this system is a great way to secure your information at the file level
- Knowing how to deploy IPSec and put it to use on a Server 2003 network is another way to keep your network as secure as possible, saving you time and money

Type of Certificate Obtained

- Windows Security Administrator

Format

- Instructor-Led Training/Classroom

Total Training Hours

- 8 hours/day

Duration

- 5-days

Language

- English

info@itsecurityct.com
www.itsecurityct.com