

## Course Introduction

Microsoft Windows Server has a large number of vulnerabilities, and supports various 'features' that can be exploited. This is a practical course where candidates learn how to remove vulnerabilities and secure these 'features' to prevent further exploits as well as techniques that hackers usually use to gain access to Windows servers.

Attendees will learn techniques how to protect windows server and audit technique which are based on global standard and best practice. The course is conducted with hands-on workshops reflect the real scenarios.

## Course Objectives

- To understand how to audit Windows server and perform auditing in a real life network
- To understand various types of risk associated with Windows based server
- To understand how to harden Microsoft Windows server
- To understand how to use security tools in Microsoft Windows server
- To understand Active directory, Group policy and apply security features into system

## Course Highlights

- Windows Software and Hardening tools include audit checklists provided
- Free membership for ACIS Alumni
  - Access to the latest information related to the course subjects
  - A life-time class re-sit

## Learning Level

- Advanced

## Course Duration

- 3 Days (18 Hours)

## Prerequisites

- TCP/IP and basic networking knowledge
- Experience implementing a Windows 2000 or Windows Server 2003 environment.
- MCSE Microsoft Certification

## Target Group

- Systems Administrators
- IT Security Officer
- IT Auditors

## Course Outline

### Module 1: General overview on Windows Servers

- Differences between Windows 2000, Windows 2003 and Windows 2008
- Server Core Installation on Windows 2008
- Basic Understanding on Active Directory System and Group Policy
- Microsoft Windows Threats
  - Threats for Windows XP ,2000 ,2003
  - Threats for Windows 7 ,2008
- LAB: Hacking Microsoft Windows
  - Information Gathering Techniques
  - Scanning Techniques
  - Enumeration Techniques
  - Password Cracking
  - Microsoft Vulnerability Exploitation

### Module 2: Security Principal

- Type of Security Principals
- Security Identifiers
  - SID Components
  - SID Authorities
  - Service SIDs
  - Well-Known SIDs

### Module 3: Windows Authentication

- Basic Authentication
- Challenge-Response Protocol
  - LM
  - NTLM
  - NTLMv2
  - Kerberos

## Module 4: Security Policies

- Local Security Policy
  - Account Policy Best Practice
  - Developing Good Auditing Policy
  - User Rights Assignment
  - Security Options
- Deploy Domain Level Security Policy using GPO
- Audit Checklist Reviews
- LAB: Hardening Windows with Microsoft Security Compliant Manager

## Module 5: Windows Firewall and Network Access Protect

- Introduction to Windows Filtering Platform (WFP)
- Managing the Windows Firewall
- IPSec Integration
- NAP Integration

## Module 6: Securing Server Roles

- Role Supported by Server Core
- OU Design for Security Policies
- GPO Design for Security Policies
- Implementing a Security Baseline
- Server Roles
  - Hardening Active Directory Domain Services
  - Hardening DHCP Services
  - Hardening DNS Services
  - Hardening Web Services
  - Hardening File Services
  - Hardening Print Services
  - Hardening Active Directory Certificate Services
  - Hardening Network Policy and Access Services
  - Hardening Terminal Services

## Module 7: Patch Management

- Introduction to Patch Management
- Microsoft Patch Management Technologies
  - Using Windows Update Stand-Alone Installer (WUSA)
  - Using Windows Server Update Services (WSUS)
- 3rd Party Patch management

## Module 8: Cryptography

- How to use EFS (Encryption File System) in detail using the Recovery Agent
- How to use Certificate Service
- What is IPSEC and how to deploy it in a windows servers
- How to use OpenSSH on Windows for Port Forwarding and other Services

## Recommended Course tracks

- PEN : Professional Penetration Testing Techniques and Vulnerability Assessment
- HDB : Hardening and Auditing Databases Security

### สำรองที่นั่งและขอรับรายละเอียดเพิ่มเติมกรุณาติดต่อ (FOR MORE INFORMATION & REGISTRATION PLEASE CONTACT)

คุณธนภัทร ไชยพิมล

Mr. Tanapat Chaipimol

Tel:(66) 2-650-5771 Ext.105 Fax: (66) 2-650 5776

Mobile: (66) 86-330-8532

Email: tanapat.ch@acisonline.net

คุณกิตมณี นิยมญาติ

Ms. Kitmanee Niyomyat

Tel:(66) 2-650-5771 ext. 108 Fax: (66) 2-650 5776

Mobile: (66) 86-325-7129

Email: kitmanee.ni@acisonline.net

### ACIS Professional Center Co.Ltd.

2101, 21 Fl., 62 The Millennia Building, Lungsuan Rd., Lumpini, Pathumwan, Bangkok 10330

Tel: +(66)2-650-5771 Fax: +(66)2-650-5776 Hotline: +(66)86-352-7129 Email: [registration@acisonline.net](mailto:registration@acisonline.net)

Website: [www.acisonline.net](http://www.acisonline.net)

