

Course Name:	Building a Secure Windows Environment
Duration:	2 Day
Medium of Instruction:	Cantonese (with terminology & handout in English)
Award of Certificate:	Certificate of Attendance

Nature and Objectives:

The widespread adoption of Microsoft Windows makes it an almost inevitable and vital core component in our IT infrastructure. Improper use of Windows will provide good opportunities for hacking activities. The course aims to equip the participants with an in-depth knowledge in deploying secure Windows environment (include Windows 2000, XP, and 2003). In addition to concept, case studies, intensive hands-on workshop will be arranged through out the course to make participants to grasp the essential knowledge for deploying a secure Windows environment (for Windows 2000, XP and 2003).

Who Should Attend:

System and Network Administrators / Engineers / Analysts, Technical Engineers / Managers, Data Security Officers, Information Security Analysts / Managers, IT Auditors and Managers, Network Managers, Security Consultants and System Integrators. Participants are expected to have hands-on experience in administering Windows 2000, XP and 2003.

Course Outline:

Common System Threats

- Current Statistics in Security Attack
- Common Windows Local Security Attack (Password guessing, sniffing, cracking)
- Remote Windows Network Security Attack (Backdoor, Trojan and Network penetration)

Basic Security Principles

- Security Enforcement Mechanisms
- Principle of Least Access
- Authorization and Authentication
- Security compliance design (e.g. ISO 27001, Orange Book, Common Criteria)
- Specific requirement before deployment

Microsoft OS Security Concepts

- OS internal design
- Security Design Concept of Windows
- Security Features in Windows XP, 2003, Win7

Identification, Authentication, Authorization and Access Control

- Secure Authentication Module
- Login Authentication and Authorization
- Credential Manager

File Systems

- File Systems Security
- Access Control setting in NTFS
- Encrypted File Systems security
- SysKey and File Systems security

System Configuration

- Bootup process
- Registry Security Setting
- Domain Controller
- Active Directory Basis
- Security for Domains, Forest, Domain Controllers and Servers

Network Configuration and Network Services

- Windows Networking design

- Remote access facilities (Terminal Server, VNC)
- IP Security, IPSec, VPN
- DNS and DHCP Security
- IIS Security

Group Security Policies

- Microsoft Network Access Protection and Quarantine Control Network
- Cisco's Network Admission Control (NAC) technologies
- Security Template Settings
- Security Configuration and Analysis Snap-in Template
- Group Policies Setting and Group Policies Object

Patches Management

- Patch arrangement in Windows Platform
- Patch management system for Windows
- WSUS and other patch management systems
- New security features in Windows

Backup and Restore

- System Backup Configuration
- System Restoration Configuration
- Automated System Recovery Configuration

Audit Logging

- Event log facilities
- Event log setting
- Event log review procedures

Other Windows Security Features

- Personal firewall
- Windows File Protection
- Software Restriction Policies and Secure Code Signing
- Spyware information
- Windows Security Essentials

Basic Forensics Investigation on Windows

- Windows Forensics Tools
- Reviewing of logs, email and recycle bin
- Windows Registry and System investigation