# HP Education Services Course Overview

Building a Secure Windows Environment (H9P50s)

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 2 days course aims to equip the participants with an in-depth knowledge in deploying secure Windows. In addition to concept, case studies, intensive hands-on workshop will be arranged throughout the course to make participants to grasp the essential knowledge for deploying a secure Windows environment.

## Audience

- System and Network Administrators / Engineers / Analysts, Technical Engineers / Managers, Data Security Officers, Information Security Analysts / Managers, IT Auditors and Managers, Network Manager, Security Consultants, and System Integrators.

## Prerequisites

- Participants are expected to have hands-on experience in administering Windows XP, 2003, 2008, 2008R2 and Windows 7.

## Why Education Services From HP?

- Hands-on practice
- Customized on-site delivery
- More than 80 training locations worldwide
- Online instructor-led and self-paced training at **www.hp.com/education**
- Comprehensive student materials
- Experienced and best-in-the-field HP instructors
- Focus on job-specific skills
- State-of-the-art classroom facilities

| | |
|---|---|
| **Course Title:** | Building A Secure Windows Environment |
| **HP Product Number:** | H9P50s |
| **Category/Subcategory:** | Information Security |
| **Course Length:** | 2 Days |
| **Delivery Language:** | English |
| **To Order:** | In HK, please contact HP Education Services on (852) 3070-6692 or email at hp-education.hk@hp.com or visit **www.hp.com.hk/education**<br>Other countries please visit **www.education.hp.com** |

## Detail Course Outline

**DAY 1 –**

**Basic Web Protocol and Attack Method**

- Statistics in Web Attack
- Basic Web Protocol (HTML, HTTP, HTML5)
- Web Architecture, web server, web proxy
- Web Authentication and Authorization Method
- Current Trend in Web Attack

**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

**Identification, Authentication, Authorization and Access Control**

- Secure Authentication Module
- Login Authentication and Authorization
- NTLM, NT GINA, Kerberos
- Credential Manager
- MIIS
- MS Passport
- Smart card usage
- UAC

**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
- Windows Integrity Control

**DAY 2 –**

**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

**Windows Virtualization**

- Hyper-V
- Virtual Server
- Application Virtualization Security

**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
- BitLocker
- Windows Powershell
- Internet Explorer 8 Security

**Code Signing**

- Spyware information

**Basic Forensics Investigation on Windows**

- Windows Forensics Tools
- Reviewing of logs, email and recycle bin
- Windows Registry and System investigation
- Basic Rules on Court accepted evidence preservation method