

Course Name:	Attacks and Defenses Warfare on Web Application Systems
Duration:	2 Day
Medium of Instruction:	Cantonese (with handout in English)
Award of Certificate:	Certificate of Attendance

Nature and Objectives:

The course presents participants with contemporary attacking techniques from sign-on to sign-off, everything in between a web-based application. It targets to help participants understand security advance in both attacking and defending sides of the “*hacking*” battlefield. Security techniques in technical, procedural and managerial aspects will be covered. This course is based on fact and experience, not theory. Much course time is allocated for hand-on exercises. On completion of the course, participants should:

- know more about technical, procedural and managerial aspects of web application security;
- know how to establish a security defended and manageable web-based architecture; and
- understand the basis of risk assessment and penetration test for web-based application.

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 and UNIX systems in a TCP/IP networking environment

Course Outline:

Basic Web Protocol and Attack Method

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

Web based information gathering

- Standard Reconnaissance Method
- Search Engine attacks
- Information Gathering through Web tools (Traceroute, OS & Application check)
- Source Code Review

Common Security Issues in Web Application

- URL Encoding Attacks
- Source Code Disclosure Attack
- File System Traversal Attacks
- Input Validation Attacks
- Web login brute-force attacks
- Web 2.0 and AJAX security

Specific Web Application Attack Method

- Impersonation Attacks
- Cookie poisoning Attack
- Cross-Site Scripting Attacks
- Session Attacks

- SQL Injection Attacks

Common Web Application Attack Tools

- Network Scanners
- Vulnerability Scanner
- Web Application Scanner
- Proxy Scanner

Secure design and implementation of Web Applications

- Secure design of Web Applications
- Web Testing security standard
- Web Security design scheme – OWASP

Securing Web Servers

- Securing of Apache Server
- Securing of IIS Server
- Use of Lockdown and Microsoft Security Configuration
- Secure ASP Development
- Secure PHP Development
- SSL Securing scheme

Securing Database Applications

- Securing of Web database security configurations
- Web database code security

Understanding Web Logs and identifying Web Attack

- Web Log formats
- Understanding Web Status Word
- Web Log analysis