

<b>Course Name:</b>	Ethical Hacking
<b>Duration:</b>	2 Day
<b>Medium of Instruction:</b>	Cantonese (with handout in English)
<b>Award of Certificate:</b>	Certificate of Attendance

### Nature and Objectives:

The course presents participants with contemporary ethical attacking techniques from perimeter to database level.

Hand on exercise will be used to supplement the concepts. On completion of the course, participants should:

- know about ethical / legal arrangement before the ethical hacking;
- know how to gather information about an Internet system;
- know how to conduct ethical hacking to network devices, Windows and Unix servers, web applications; and
- know about automated tools to help identify problematic codes in code review.

### 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 basic understanding in system and network administration in a TCP/IP networking environment.

### Course Outline:

#### Introduction to Ethical Hacking

- Types of External Attacks
- Vulnerability Research
- Cyber Law
- Computer Crimes and Implications
- System Hacking Cycle

#### Virus, Trojans and Rootkits

- Virus, Worms, Trojans
- Rootkits and Malware
- Microsoft Windows Defender
- Hardware and Software Threats
- Anti-Virus Software
- Effectiveness of the Anti-Virus Packages

#### Information Gathering

- Host and Network Foot Printing
- Enumerating Remote Systems
- Google Hacks
- Using Google as a Proxy Server
- Google Hacking Database (GHDB)
- Anonymity with Caches
- Locating Public Vulnerable Targets

#### Host Enumeration

- Techniques for Enumeration
- NetBIOS Null Sessions
- Services enumeration

#### Host Scanning

- Types and Objectives of Scanning
- Network discovery
- Banner Grabbing
- Enumerate Web Application
- Vulnerability Scanning

#### Vulnerability Scanners

- Online vulnerability search engine
- NMap, Nessus, OpenVAS and others port and vulnerability scanners

#### Web Application Security

- Web server fingerprinting
- Cross-Site Scripting
- Session Hijack
- SQL Injection
- Parameter/Form Tampering
- Hidden Field
- Buffer Overflow
- Directory Listings and Traversal Techniques
- Cryptographic Interception
- Cookie Snooping
- Authentication Hijacking
- Log Tampering
- Error Message Interception

#### Code Review

- Common Vulnerabilities in Code
- Code Review tools for Common Programming Languages

#### Packets Sniffing

- TCPDump, Windump and Wireshark
- Cain and Abel
- ARP Spoofing
- DNS Poisoning Techniques
- TCP Relay Replay Attacks
- How to Detect Sniffing

#### System Hacking Techniques

- Cracking Password
- Escalating Privileges
- Executing applications
- Hiding files
- Covering Tracks

#### Miscellaneous

- Denial of services
- Peer-to-Peer Applications
- Instant Messaging
- SANS Top-20 Internet Security

➤ Attack Targets and OWASP Top 10