

<b>Course Name:</b>	Assessing Network Vulnerabilities
<b>Duration:</b>	2 Day
<b>Medium of Instruction:</b>	Cantonese (with terminology & handout in English)
<b>Award of Certificate:</b>	Certificate of Attendance

### Nature and Objectives:

Security professionals are overwhelmed by abundant security advisories, intrusion and firewall alerts, and vulnerability reports. Knowledge of actual hacking techniques and scenarios permits a more effective response against the growing threats from Internet access and presence. The course teaches participants how to exploit and run vulnerability scans to better secure networks, servers and workstations. In the course, you will learn how to

- Assess the risk to your systems from vulnerabilities and exploits
- Employ exploits to validate system defenses
- Conduct vulnerability scans of your networks, servers and workstations
- Integrate advisories and alerts into your security practices and procedures
- Respond to evolving risk levels by prioritizing your defensive resources
- Manage ongoing vulnerability assessment

### Who Should Attend:

System and Network Administrators / Engineers / Analysts, Technical Engineers / Managers, Data Security Officers, Information Security Analysts / Managers, IT Auditors & Managers, Network Managers.

### Course Outline:

#### Network Security Assessment

- The challenge of today information security
- The business benefits
- Threats, vulnerabilities, and attacks
- Policy formulation and implementation
- The assessment approach

#### Networking and Systems Review

- Ethernet, TCP/ IP security
- Network and Internet Services
- Firewalls, Intrusion Detection
- Intrusion Prevention Systems
- Common Operating Systems

#### Common Vulnerabilities

- Workstation and Server vulnerabilities
- Web Server, Database server, Mail server, Web server, DNS server
- Server vulnerabilities, Malware: Virus, Worms, Adware, Spyware, Keylogger

#### Web Application Vulnerabilities

- Cross site scripting (XSS)
- SQL injection

#### Information Gathering

- Web Search Engines
- DNS Querying and digging
- Company Website
- Tools, Techniques and Methodology
- Reconnaissance
- Social Engineering

#### Assessment Tools

- The operating systems
- Free network scanning tools

- Commercial scanning tools

- Other assessment tools

#### Common Network Attacks

- DoS & DDoS
- Password Cracking
- Password Brute Force attack test
- Trojan Horses & Back-Doors
- IP Spoofing, Session Hijacking
- Traffic interception, and Traffic manipulation (Man- In-The-Middle attack)

#### External and Internal Penetration Test

- ICMP Probing (Ping & Traceroute)
- NMap OS Fingerprinting Scanning
- OS Fingerprinting
- TCP and UDP port scanning techniques
- Service Banner Grabbing
- E-Mail header analysis
- System Services Identification
- Automated Scanning

#### Exploitation Fundamentals

- Buffer overflows, Heap overflows
- Format string, Race condition
- Local exploits, remote exploits

#### System Exploits

- SMB, RPC, Privilege escalation
- Covering tracks, Log file eraser, Covert file hiding
- How Shellcode Works
- Maintaining Access after Break-in
- Rootkits, Covert communication