

<b>Course Name:</b>	Securing Your Corporate Network Infrastructure
<b>Duration:</b>	3 Day
<b>Medium of Instruction:</b>	Cantonese (with handout in English)
<b>Award of Certificate:</b>	Certificate of Attendance

### **Nature and Objectives:**

The 3-day intensive hands-on workshop aims to equip participants with a comprehensive understanding of the security issues in a corporate network infrastructure environment. It is designed to help network and security professionals to further understand the various aspects of network and system security. The course will also highlight how a hacker thinks and works. The participants would then be able to defend his network and system. Each participant will be provided with an environment to practice prevention measures against subversive attacks and intrusions. There will be exercises in which the participants are expected to try out related techniques.

### **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.

### **Course Outline:**

#### **Common Network Threats & Cyber Attacks**

- Cyber Stalking, Cybercrime, Cyber Terrorism & Identity Theft
- Network Probing, Packet Sniffing, Password Eavesdropping & TCP/IP Attacks
- Email Attacks (Spoofing, Phishing, Pharming & Spamming)
- DoS and DDoS Attacks
- Web Service and Web Application Attacks
- Viruses, Worms & Malware Attacks

#### **Secure Network Architecture Design**

- Principles & Approaches
- Network Components and Architecture
- Demilitarize Zone & Private Zone (Network Isolation)

#### **Advanced Security Considerate of Network Components**

- Routers and Switches
- Virtual Local Area Network (VLAN)
- Advanced Application of Firewalls
- Intrusion Detection & Prevention
- Virtual Private Network (VPN)
- Monitoring & Auditing Systems

#### **Advanced Wireless Network Security**

- Wireless Network Architecture
- Wireless Security Threats & Mitigation
  - Assessing WLAN vulnerabilities
  - Peer attacks & Information Theft
  - Forcing client de-authentication
  - Intercepting Wi-Fi traffic
  - RF Jamming & Data Flooding

#### **Systems Hardening**

- Principles & Approaches
- Systems Architecture & Configuration
- Network Components
- Operating Systems

- Applications
- Services

#### **Passive Vulnerability Discovery**

- Internet Profiling and Information Gathering
- Online Tools
- Google Hacking
- Footprint Analysis

#### **Active Vulnerability Discovery**

- Penetration Testing
- Vulnerability Assessment
- Firewall and VPN Assessment
- Server Configuration Assessment
- Network Architecture Assessment
- Web Vulnerability Scanning
- Web Applications Assessment
- Wireless Security Assessment
- VoIP Security Assessment
- Social Engineering

#### **Protection for Data Transmission**

- Cryptography for Data Transfer
- Secure Remote Access

#### **Data Protection & Access Control**

- Wireless Devices Security
- Extensible Authentication Protocol
- VPN technologies in Legacy WLAN
- Deploy & Control Advance WLAN

#### **Resilience, High Availability and Disaster Recovery**

- Models of Redundancy
- Clustering & Load Balancing
- Control Measures in DR Plan
- Strategies of Disaster Recovery