

Course Name:	Linux / Unix Security
Duration:	2 Day
Medium of Instruction:	Cantonese (with terminology & handout in English)
Award of Certificate:	Certificate of Attendance

Nature and Objectives:

The widespread adoption of Linux / Unix makes it an almost inevitable and vital core component in our IT infrastructure. Improper use and configuration of the operating systems will provide good opportunities for hacking activities. The course aims to equip the participants with an in-depth knowledge in deploying secure common Linux / Unix operating systems. In addition to concept, case studies, intensive hands-on workshop will be arranged through out the course to make participants to grasp the essential knowledge.

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:

Introduction to UNIX/Linux Operating Systems

- Security Principles
- Security Considerations
- Vulnerabilities, Threats and Risks
- BIOS Security
- Harddisk Partitioning
- Boot Loader Security
- Inittab and Boot Scripts
- Post-installation Hardening

Users & Groups Access Controls

- Managing User and Group
- User Accounts access controls
- Displaying Login Banners
- Restricting Direct Login Access
- Replacing Telnet, rlogin and
- Password Security and Encryption
- Pluggable Authentication Module
- Standard Authentication Modules

Securing File System

- File and Directory Permissions
- File system Mount Options
- NFS Properties and rhost
- Policies, & Configuration
- File Encryption

Securing Services

- Service Discovery, Minimization
- FTP, Telnet, OpenSSH
- Domain Name Service

- Mail Service

- Web Server

Maintaining System Security

- Package management: RPMs, dbpk, apt-get, YaST
- System Logging and Audit Trails
- Patching Linux Systems
- Backup and Restore
- Secure Time Synchronization

Secure Common Services

- Scanning and Mapping Vulnerabilities
- Services Probing
- Services and Vulnerability Scanner

UNIX/Linux Network Protections

- Packet Sniffing
- Access Control List
- TCP Wrappers
- Restricting System Access from Networks
- VPNs - Virtual Private Networks
- IPTables Firewall

SELinux

- DAC vs. MAC Security
- Shortcomings of Traditional UNIX Security
- SELinux Goals, Terms, and Architecture
- Activating and Interfacing with SELinux
- SELinux commands and Roles
- Understanding and Modifying Policy Source
- File Context Files (*.fc)
- Policy Analysis & Customization