Progettare e realizzare la sicurezza di Sistemi Operativi Microsoft Windows

Il rischio di vulnerabilità di sistemi Windows può essere notevolmente ridotto con una opportuna configurazione del sistema. Mentre alcuni accorgimenti dovrebbero essere presi in ogni situazione, la configurazione più adatta a mettere in sicurezza un sistema in ogni contesto di esercizio deve essere valutata di caso in caso. Per raggiungere questo livello di abilità, è necessario conoscere in dettaglio il progetto e l'implementazione della sicurezza di sistemi basati su piattaforme Windows Server e Client.

Agenda (5 giorni)

Funzionalità e strumenti di sicurezza base dei sistemi operativi Windows.

Richiami sul modello di sicurezza nei sistemi Windows:

- gestione delle utenze, dell'autenticazione, dell'autorizzazione, Access Control List
- sicurezza del file system, dei processi, del sottosistema I/O, del sistema di memory management.

Tecniche tradizionali di intrusione nel sistema:

- cracking delle password ed impersonamento; Virus e minacce correlate; Memory leak e Buffer overflow.

Richiami sul modello di sicurezza distribuita nei sistemi Windows:

- implementazione e configurazione del TCP/IP e del Netbios Windows
- servizi di rete base del S.O. (RPC; Servizi di naming: NetBios e DNS; File Sharing, Distributed File Sharing e Print Sharing; Web Server: IIS; Remote Control di sistemi Windows)
- gestione distribuita delle utenze (Domain Controller, Active Directory) e configurazioni avanzate del sistema di autenticazione e autorizzazione
- rilevazione delle intrusioni tramite logging e auditing
- l'event viewer di Windows
- tecniche di rilevazione statistica delle intrusioni: strumenti di monitoraggio statistico e real time del sistema
- software di intrusion detection
- tecniche di rilevazione basate su regole: utilizzo di firewall locali.

Hardening e Policy Compliance: Windows Domain e Group Policy; Network Access Protection.

Protezione dei dati e delle comunicazioni:

- utenti mobili e BIT Locker
- cifrare le comunicazioni con i certificati
- Remote Access in SSL VPN
- Windows Direct Access.

Soluzioni e architetture di prodotti anti virus: trade-off nelle prestazioni di sistemi protetti da sistemi antivirus.

Dimostrazioni e esercitazioni.

Analisi della configurazione di prodotti: per la difesa/attacco di un sistema: Sniffer, Spoofer, Portscanner per l'hardening di un sistema operativo in libera distribuzione: software di firewalling per la cifratura e la firma di posta elettronica: configurazione ed uso di certificati digitali con Netscape, MS-Explorer, MS-Outlook.

Obiettivi

Al termine del corso i partecipanti hanno conoscenze in dettaglio e competenze per configurare e gestire la sicurezza dei sistemi operativi Windows, sia stand alone che nelle più complesse configurazioni in rete.

Destinatari

Responsabili di S.I., CED e di infrastrutture di rete, Progettisti e amministratori di sistemi di rete, Consulenti junior di Security management, Sistemisti di rete, Supervisori di sistemi di sicurezza.

Prerequisiti

Buona conoscenza dei sistemi operativi Windows, delle reti di computer, della suite di protocolli TCP/IP e conoscenza di base sulla amministrazione di sistemi informativi complessi.

Quota di iscrizione	*Informazioni*
€ 2.240,00 (+ IVA) *(Comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione).*	Segreteria Corsi – Reiss Romoli s.r.l. tel 0862 452401 - fax 0862 028308 corsi@ssgrr.com