La sicurezza nei Sistemi operativi UNIX/Linux

I rischi di vulnerabilità di sistemi Unix può essere notevolmente ridotto con una opportuna configurazione del sistema stesso. 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 Unix.

Agenda (4 giorni)

Funzionalità e strumenti di sicurezza base dei sistemi operativi Unix/Linux.

Richiami sul modello di sicurezza nei sistemi Unix/Linux:

gestione di: utenze, autenticazione, autorizzazione; Access Control List
sicurezza di: file system, processi, sottosistema I/O e sistema di memory management.

Tecniche di intrusione nel sistema:

cracking delle password ed impersonamento
memory leak
buffer overflow.

Richiami sul modello di sicurezza distribuita nei sistemi Unix/Linux.

Personalizzazioni del kernel per attuare le contromisure.

Implementazione e configurazione del TCP/IP.

Servizi di rete base del S.O.:

servizi di identificazione; SMTP; File Sharing; Web Server; esportazione del display
gestione distribuita delle utenze: NIS/NIS+. YP
gestione delle utenze delle applicazioni di rete: mail, web.

Rilevazione delle intrusioni tramite logging e auditing:

standard syslog
tecniche di rilevazione statistica delle intrusioni:strumenti di monitoraggio statistico e real time
software di intrusion detection
tecniche di rilevazione e filtraggio basate su regole (Linux):Ipchain/Iptables.

Esercitazioni:

analisi della configurazione di prodotti per la difesa/attacco di un sistema:Sniffer, Spoofer, Portscanner
analisi della configurazione di prodotti per l'hardening di un sistema operativo
strumenti per la verifica della tenuta di Firewall e strumenti IDS.

Analisi della configurazione di prodotti per la implementazione di SSL ed HTTPS:

configurazione di un client e di un server.

Obiettivi

Il corso è finalizzato ad acquisire le competenze per la configurazione e gestione della sicurezza dei S.O. Unix/Linux, sia stand alone sia nelle più complesse configurazioni in rete.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenza di base di S.O., reti di computer, suite di protocolli TCP/IP e della amministrazione di sistemi informativi complessi.

Iscrizione

Quota di Iscrizione: 1.980,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com