Reti sicure in ambiente Cisco, difesa perimetrale con IOS Firewall

Il corso presenta le varie tipologie di attacco a cui può essere sottoposta una rete enterprise e le tecniche atte a mitigare tali attacchi attivando le funzionalità di sicurezza che sono presente nei sistemi operativi dei router e degli switch: controllo degli accessi, firewall ed IPS. Inoltre, essendo le reti enterprise geografiche sempre più spesso realizzate utilizzando backbone IP, il corso illustra come mettere in sicurezza le reti usando le reti private virtuali.Per ciascuna soluzione vengono valutati gli aspetti di sicurezza e le metodologie pratiche di messa in sicurezza degli apparati costituenti la rete, con particolare riferimento agli apparati Cisco. Il corso prevede, oltre alla descrizione teorica degli argomenti trattati, una rilevante attività di laboratorio 'hands on' su un ricco laboratorio, costituito da router e switch Cisco, nel quale sono riprodotte situazioni analoghe a quelle reali. Oltre alle operazioni di configurazione saranno effettuate esercitazioni che, partendo da reti già configurate, mirano ad aggiungere servizi/applicazioni ed a modificare le configurazioni dei dispositivi per conseguire miglioramenti nella sicurezza della rete.

Agenda (5 giorni)

Sicurezza a livello di data link:

tipi di attacchi
come mitigare gli attacchi
mettere in sicurezza il layer 2: PVLAN, controllo del DHCP e dell'ARP.

Gestione degli accessi alla rete: 802.1X.

Network Foundation Protection: mettere in sicurezza il piano dati, gestione e controllo.

Dispositivi di Sicurezza nei router Cisco:

Network address translation
Cisco IOS Firewall
implementazione e configurazione di Cisco IOS firewall in modo classico (interface-based)
implementazione e configurazione di Cisco IOS firewall basato sulle zone (zoned-based)
configurare l'Authentication Proxy
Cisco IOS IPS
implementazione e configurazione di Cisco IOS IPS.

Reti Private Virtuali:

il protocollo IPSec
implementazione di VPN IPSec con pre-shared keys e con PKI
implementazione di VPN IPSec facilmente scalabili
configurazione di Tunnel GRE su IPSec
configurazione di VPN su più siti, Dynamic Multipoint VPN
configurare VPN altamente affidabili
implementare l'accesso remoto
configurazione di VPN SSL
configurazione di Easy VPN.

Obiettivi

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.

Iscrizione

Quota di Iscrizione: 2.400,00 € (+ 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