CCNA Security

corrisponde a Implementing Cisco IOS Network Security (IINS)

Il corso CCNA Security fornisce le competenze necessarie per amministrare in sicurezza una rete IP di medie dimensioni sia in ambito LAN che WAN. L'obiettivo del corso è quello di preparare i partecipanti a diventare delle figure professionali in grado di sviluppare una infrastruttura sicura di rete, di valutare le vulnerabilità della propria rete e di mettere in campo le opportune misure per contrastare le possibili minacce. Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco 210-260 IINS v3.0.

Agenda (5 giorni)

Le componenti tecniche del "Sistema-Sicurezza":

disponibilità, integrità (autenticità, non-ripudio), riservatezza
sicurezza logica: servizi di sicurezza, tipologia degli attacchi, anatomia di un attacco
certificare la sicurezza (ISO 27000 e ISO 15408).

Esaminare le tipologie di attacco e minimizzare la probabilità di successo dell'attacco:

mitigare gli attacchi di accesso abusivo
attacchi basati sulle password
sfruttamento della fiducia (trust exploitation)
redirezione delle porte
mitigare gli attacchi di Buffer Overflow
IP Spoofing
attacchi DoS e DDoS
virus, worm, e trojan horse
attacchi a livello applicativo
protocolli di gestione
attacchi di raccolta delle informazioni (reconnaissance)
packet sniffer; port scan e ping sweep; query alla Internet pubblica.

Rendere sicuro l'accesso amministrativo degli apparati di rete:

configurare la password
creazione di un account utente
configurare Role-Based CLI access
configurare il supporto avanzato per Virtual Login.

Sicurezza nei router Cisco:

come mettere in sicurezza il piano dei dati, di controllo e di management
descrivere Cisco Security Manager
descrivere le implicazioni che IPv6 introduce nel campo della sicurezza.

Configurare AAA sui Router Cisco usando il database locale:

descrivere le funzioni e l'importanza di AAA
conoscere come i servizi di AAA (Authentication, Authorization, Accounting) sono supportati in Cisco IOS software
conoscere come rendere sicuro l'accesso ai dispositivi di rete e alle reti
configurare AAA con un database locale.

Configurare AAA con l'ausilio di Cisco Secure ACS:

comprendere i benefici di un AAA centralizzato
conoscere le caratteristiche di Cisco Secure Acces Control Server (ACS)
conoscere le caratteristiche dei protocolli RADIUS e TACACS+
installare e configurare il server ACS
configurare i protocolli RADIUS e TACACS+
verificare l'operatività di AAA (troubleshooting).

Liste di accesso:

access control lists (ACL)
standard IP ACL e Extended IP ACL
gestione avanzata delle ACL
configurare e verificare le ACL.

Gestione sicura degli apparati e monitoraggio:

gestione In-Band e Out-Band

linee guida generali sul Management e Reporting in sicurezza
usare i log per monitorare la sicurezza della rete; modelli e livelli di sicurezza di SNMP
Secure Shell (SSH).

Attacchi a livello 2:

proteggere le funzionalità di inoltro degli switch: MAC flooding, MAC spoofing
port security
prevenire il VLAN hopping: switch spoofing, doppio tag
prevenire le manipolazioni dello STP: BPDU guard, root guard, BPDU filtering
proteggere il DHCP
Private VLAN
monitoraggio su reti switched (SPAN: Switched Port Analyzer).

Tecnologie di firewalling:

soluzioni per la difesa del perimetro della rete aziendale
funzionalità di un firewall: packet filtering, proxy, statefull inspection
funzionalità complementari
architetture firewall: screened host, screened network o subnet (DMZ)
tipi di NAT usati nei firewall
configurare Network Address Translation (NAT) e Port Address Translation (PAT)
configurare Cisco IOS Zone-Based Policy Firewall usando CCP (Cisco Configuration Professional)
case studies su Zone-based firewall
apparati Cisco di firewalling: Adaptive Security Appliance (ASA).

Cisco IPS:

descrivere le funzioni di Cisco Intrusion Prevention System (IPS)
tecnologie IPS: Profile-based, Signature-based, Protocol-based
mitigazione delle minacce su un sistema distribuito utilizzando IPS
configurare Cisco IOS IPS usando CCP (Cisco Configuration Professional).

IPSec e VPN:

strumenti per la sicurezza dei dati, crittografia pratica
crittografia simmetrica o a chiave segreta crittografia asimmetrica o a chiave pubblica funzioni di hashing (MD5, SHA-1) ed HMAC
certificati Digitali e PKI
reti private virtuali (RPV o VPN): tipi e tecnologie
componenti e funzionalità di IPSec: AH, ESP e IKE
configurare IPSec site-to-site con chiavi precondivise
verificare l'operatività delle VPN
realizzare VPN con Secure Sockets Layer (SSL).

Simulazione dell'esame e test di preparazione.

Obiettivi

Fornire le conoscenze e competenze necessarie per l'installazione, la gestione ed il troubleshooting dei dispositivi di rete garantendo il mantenimento dell'integrità, della disponibilità e della riservatezza delle informazioni gestite dalla rete.

Destinatari e Prerequisiti

A chi è rivolto

Tecnici (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'integrazione e della configurazione di reti IP che vogliono minimizzare l'impatto che malfunzionamenti, provocati o accidentali, possono causare sulla propria rete IP.

Prerequisiti

Sono richieste nozioni sull'internetworking simili a quelle fornite nel corso CCNA: conoscenze sui concetti e i termini legati al mondo del networking e dell' IP, conoscenza del mondo LANs, WANs, e IP switching/ routing, capacità di configurare un router e uno switch con la CLI.

Iscrizione

Quota di Iscrizione: 2.300,00 € (+ IVA)

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

Quota di Iscrizione comprensiva del Voucher: 2.528,00 € (+ IVA)

Con l'acquisto del voucher è possibile sostenere l'esame di certificazione.

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

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

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