

Formation IPv6: Sécurité professionnelle IPv6 (IPv6SECFR, 4 jours)

Description

Le cours Sécurité professionnelle IPv6 (formation IPv6) aborde tous les aspects de la sécurité IPv6, des bases de la pile de protocoles IPv6 aux vulnérabilités des protocoles et des applications. En commençant par un examen de l'adressage IPv6, le cours présente aux participants toute la gamme des vulnérabilités et des contre-mesures de sécurité. Nous abordons, entre autres, le DHCPv6 avec et sans état, le DNSv6, ICMPv6 et IGMPv6. Le cours explore également les protocoles de routage, les ACL, les VLAN, les pare-feu, la VOIP, la mobilité IPv6 et plus encore.

Tarifs

- Tarification: \$3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Examen des principes fondamentaux d'IPv6

Principales différences entre IPv4 et IPv6

Comprendre l'espace d'adressage IPv6

Comprendre les types d'adresses IPv6

Expression de l'adresse IPv6

Comprendre l'autoconfiguration sans état et avec état'.

Comprendre le DHCPv6

L'en-tête IPv6

Comprendre les extensions d'en-tête

Comprendre la découverte des voisins

Exploration de ICMPv6

Comprendre le DNSv6

Un regard rapide sur le trafic de bout en bout dans un réseau IPv6

Un tour rapide de la coexistence d'IPv4 et d'IPv6

Introduction à la sécurité d'IPv6

Réintroduction d'IPv6

Mise à jour de l'IPv6

Vulnérabilités IPv6

Expérience des hackers

Techniques d'atténuation de la sécurité d'IPv6

Lectures et ressources recommandées

Vulnérabilités de la sécurité du protocole IPv6

L'en-tête du protocole IPv6

Menaces sur les en-têtes d'extension

Reconnaissance sur les réseaux IPv6

Spoofing des couches 3 et 4

Sécurité de l'Internet IPv6

Menaces Internet à grande échelle

Filtrage des entrées/sorties

Sécurisation des sessions BGP

Sécurité d'IPv6 sur MPLS

Équipement des locaux du client

Menaces de délégation de préfixe

Questions relatives au multihébergement

Sécurité du périmètre IPv6

Pare-feu IPv6

ACL de routeur Cisco IOS

Pare-feu Cisco IOS

Pare-feu Cisco PIX/ASA/FWSM

Sécurité des réseaux locaux

Pourquoi la couche 2 est importante

Vulnérabilités de la couche 2 d'ICMPv6 pour IPv6

Protection du protocole ICMPv6

Détection par le réseau des attaques ICMPv6

Atténuation du réseau contre les attaques ICMPv6

Adresses d'extension de la confidentialité pour le meilleur et pour le pire

Menaces et atténuation de DHCPv6

Liaison point à point

Sécurité des points d'extrémité

Renforcement des dispositifs réseau IPv6

Menaces contre les dispositifs de réseau

Versions de Cisco IOS

Désactiver les services réseau inutiles

Limiter l'accès au routeur

Gestion des dispositifs IPv6

Menaces contre le protocole de routage intérieur

Sécurité du protocole de redondance de premier saut

Contrôle des ressources

Menaces sur la QoS

Sécurité des serveurs et des hôtes

Sécurité des hôtes IPv6

Pare-feu de l'hôte

Sécurisation des hôtes avec Cisco Security Agent

Réseaux privés virtuels IPsec et SSL

Sécurité IP avec IPv6

IPsec hôte à hôte

Configuration IPsec site à site

Accès à distance avec IPsec

VPN SSL

Sécurité pour la mobilité IPv6

Fonctionnement de l'IPv6 mobile

Messages MIPv6

Menaces liées à MIPv6

Utiliser IPsec avec MIPv6

Filtrage pour MIPv6

Autres protocoles de mobilité IPv6

Sécurisation des mécanismes de transition

Attaquer le NAT-PT

Menaces latentes d'IPv6 contre les réseaux IPv4

Surveillance de la sécurité

Gestion et surveillance des réseaux IPv6

Gestion des tunnels IPv6

Utilisation de la criminalistique

Utilisation des systèmes de détection et de prévention des intrusions

Gérer les informations de sécurité avec CS-MARS

Gestion de la configuration de la sécurité

Conclusions sur la sécurité IPv6

Comparaison des sécurités IPv4 et IPv6

Modification du périmètre de sécurité

Création d'une politique de sécurité IPv6

À l'horizon

Liste des recommandations