IPV6, SÉCURITÉ

Public	Ingénieurs réseau/sécurité chargés de l'étude ou du déploiement d'un réseau IPv6.
Durée	2 jours - 14 heures
Pré-requis	Connaissances équivalentes à celles apportées par le stage "IPv6, mise en œuvre".
Objectifs	Connaître les problèmes de vulnérabilité liés à la mise en œuvre d'IPv6 Mettre en œuvre les solutions de sécurité appropriées Appliquer les bonnes pratiques de sécurité
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

1. INTRODUCTION À LA SÉCURITÉ SOUS IPV6

- Le protocole IPSec.
- L'authentification des hôtes avec AH.
- La confidentialité des données avec ESP.
- Le mécanisme d'échange de clés IKE.

2. LES VULNÉRABILITÉS LIÉES À L'AUTOCONFIGURATION SANS ÉTAT (RA)

- Les mauvaises pratiques fréquentes. Les problèmes liés aux mauvaises pratiques.
- Les attaques de dénis de service (DOS).
- Les techniques de "Man In The Middle".

3. VULNÉRABILITÉS DES FONCTIONNALITÉS DES PROTOCOLES IPV6/ICMPV6/AUTOCONF

- L'usurpation d'adresse.
- L'utilisation des messages ICMP redirect.
- Le bon usage des filtrages d'ICMPv6.
- Le contrôle des identifiants d'interface.
- Les adresses anycast.
- IPv6 et les extensions.

4. LES VULNÉRABILITÉS LIÉES AUX SERVICES RÉSEAUX

- DHCPv6 : risques liés à son utilisation.
- DNS et IPv6 : les bonnes pratiques.

5. LES VULNÉRABILITÉS LIÉES AUX TUNNELS

- Contrôle de son interconnexion.
- Se croire à l'abri d'IPv6.

6. LES BONNES PRATIQUES DE CONSTRUCTION DE RÉSEAU

- L'utilisation des adresses de type ULA.
- Le filtrage de trafic.

7. CONTRÔLE DES APPLICATIONS

- Le contrôle des adresses et des ports en écoute.
- Le contrôle des abonnements aux groupes multicast.

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation