IPv6, sécurité

-Réference: **PL-57** -Durée: **2 Jours (14 Heures)**

Les objectifs de la formation

- Connaître les problèmes de vulnérabilité liés à la mise en oeuvre d'IPv6 Mettre en oeuvre les solutions de sécurité appropriées Appliquer les bonnes pratiques de sécurité

A qui s'adesse cette formation ?

POUR QUI :

- Ingénieurs réseau/sécurité chargés de l'étude ou du déploiement d'un réseau IPv6.

Programme

- **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.
  - Travaux pratiques Mise en oeuvre d'IPSec en mode transport entre deux hôtes.
  - Déploiement d'un tunnel IPsec entre deux routeurs.
- **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".
  - Travaux pratiques Mise en évidence des problématiques, suivie de mise en oeuvre de solutions sur les switchs et les machines.
- **Vulnérabilités des fonctionnalités des protocoles IPv6/ICMPv6/autoconf**
  - L'usurpation d'adresse.
  - L'utilisation des messages ICMP redirect.

Programme

- Le bon usage des filtrages d'ICMPv6.
- Le contrôle des identifiants d'interface.
- Les adresses anycast.
- IPv6 et les extensions.
- Travaux pratiques Mise en évidence des risques, suivie de mise en oeuvre de solutions sur les switchs et les machines.

- **Les vulnérabilités liées aux services réseaux**
  - DHCPv6 : risques liés à son utilisation.
  - DNS et IPv6 : les bonnes pratiques.
  - Démonstration Illustrations des risques liés à l'utilisation de DHCPv6.
  - Discussions sur les bonnes pratiques liées au DNS et IPv6.
- **Les vulnérabilités liées aux tunnels**
  - Contrôle de son interconnexion.
  - Se croire à l'abri d'IPv6.
  - Démonstration Illustration par des exemples des risques associés aux tunnels.
- **Les bonnes pratiques de construction de réseau**
  - L'utilisation des adresses de type ULA.
  - Le filtrage de trafic.
  - Travaux pratiques Mise en oeuvre de filtrage sur les routeurs.
  - Discussions sur les bonnes pratiques.
- **Contrôle des applications**
  - Le contrôle des adresses et des ports en écoute.
  - Le contrôle des abonnements aux groupes multicast.
  - Travaux pratiques Analyse sous Windows et Unix.
  - Mise en oeuvre de filtrage sur les machines.

(+212) 5 22 27 99 01

(+212) 6 60 10 42 56

Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7éme étage N° 30
Casablanca 20340, Maroc