IPv6, sécurité

Cours Pratique de 2 jours - 14h
Réf : VCR - Prix 2024 : 1 760CHF HT

Cette formation vous apprend à mettre en œuvre IPv6 en toute sécurité. Vous y verrez les vulnérabilités d'IPv6 à différents niveaux, les solutions concrètes appropriées et les bonnes pratiques liées à la mise en œuvre du réseau. Un panorama complet pour être plus rapidement opérationnel.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

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

Pédagogie active basée sur des échanges, des exemples, des exercices pratiques et une évaluation tout au long de la formation.

MISE EN SITUATION

Démonstration des différents types de problèmes et mise en œuvre pratique des solutions appropriées.

PARTICIPANTS

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

PRÉREQUIS

Connaissances équivalentes à celles apportées par le stage "IPv6, mise en œuvre" (réf. PVI).

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 04/2022

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.

Travaux pratiques : Echanges. Mise en œuvre d'IPSec en mode transport entre deux hôtes. Déploiement d'un tunnel IPsec entre deux routeurs.

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".

Travaux pratiques : Mise en évidence des problématiques, suivie de mise en œuvre de solutions sur les switchs et les machines.

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.

Travaux pratiques : Mise en évidence des risques, suivie de mise en œuvre de solutions sur les switchs et les machines.

4) 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.

5) 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.

6) Les bonnes pratiques de construction de réseau

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

Travaux pratiques : Mise en œuvre de filtrage sur les routeurs. Discussions sur les bonnes pratiques.

7) 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 œuvre de filtrage sur les machines.

LES DATES

CLASSE À DISTANCE
2024 : 23 sept.