Juniper, sécurité

Cours Pratique de 3 jours
Réf : JUS - Prix 2022 : 2 190€ HT

Ce stage vous montrera comment mettre en œuvre les principaux moyens de sécurisation des systèmes et des réseaux à l'aide de routeurs pare-feu Juniper. Vous apprendrez le rôle des équipements de sécurité dans la protection de l'entreprise afin d'être en mesure de concevoir une architecture de sécurité.

OBJECTIFS PÉDAGOGIQUES

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

Identifier le rôle des divers équipements de sécurité

Mise en œuvre de tunnels IPSec

Configurer et surveiller des zones multiples

Configurer l'authentification par un pare-feu

LE PROGRAMME

dernière mise à jour : 06/2021

1) Introduction à la sécurité des réseaux

- Le vocabulaire de la sécurité informatique.
- Routage traditionnel, vulnérabilités.
- Sécurité traditionnelle avec pare-feu séparé, NAT/PAT, VPN.
- Nouvelle approche : ramasser la DMZ en une seule machine avec le concept SRX.
- La solution de sécurité proposée par Juniper Networks avec la famille SRX.

2) Les zones de sécurité

- Définition et principe des zones.
- Zones de sécurité, zones fonctionnelles. Configuration des zones.
- Monitoring des zones et du trafic.

Travaux pratiques : Configuration et surveillance de zones multiples.

3) Politiques de Sécurité (Security Policy)

- Définition d'une policy, composants.
- Déclenchement et vérification des policy.
- Etude de cas d'usage de policy.

Travaux pratiques : Mise en œuvre de policy entre les zones, filtrant plusieurs services dont FTP.

4) Authentification à travers un pare feu

- Problématique de l'authentification.
- Authentification transversale (passthrough).
- Authentification par portail captif, groupes de clients.
- Usage de serveurs externes d'authentification.

Travaux pratiques : Configuration d'authentification par pare-feu.

5) Filtrage propriétaire de risques connus : SCREEN

- Description des classes d'attaques et leurs différents niveaux d'application.

PARTICIPANTS

Techniciens et administrateurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances en réseaux et systèmes.

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.

- Revue des différents types d'attaque et leurs parades : reconnaissance, DoS, Packet attacks.
- Configuration des options de SCREEN.
Travaux pratiques : Implémentation des options de screening et test.

6) Network Address Translation

- Présentation générale du NAT.
- NAT Source : opération et configuration.
- NAT Destination : opération et configuration.
- Le Proxy ARP.
- Vérification de l'opération de NAT.
Travaux pratiques : Pratique de NAT source par interface et par pool, pool-based destination NAT.

7) Introduction aux IPSec VPN, IDS/IPS

- Définition des VPN, exigences de sécurité, principes généraux.
- Architecture d'IPSec.
- Configuration de base IPSec et Monitoring.
- Présentation de la Prévention et détection d'intrusion (IDS/IPS).
Travaux pratiques : Mise en œuvre de tunnels IPSec.

LES DATES

CLASSE A DISTANCE

2022 : 03 oct.