Formation : PKI, mise en œuvre

Cours pratique - 4j - 28h00 - Réf. PKI
Prix : 2960 CHF H.T.

4,4 / 5

BEST

Ce cours vous montrera comment mener un projet Public Key Infrastructure (PKI) dans les meilleures conditions. Les travaux pratiques vous apprendront à déployer une autorité de certification, à générer des certificats et à mettre en œuvre une messagerie sécurisée et une solution Single Sign-On (SSO).

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Appréhender les différents algorithmes de chiffrement symétrique et asymétrique
- Mettre en œuvre une hiérarchie d'autorités de certification
- Mettre en œuvre une messagerie sécurisée
- Mettre en œuvre une authentification forte par certificat X509

Public concerné

Ingénieurs, administrateurs systèmes et réseaux.

Prérequis

Bonnes connaissances en systèmes, réseaux et sécurité informatique.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

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.

Programme de la formation

PARTICIPANTS

Ingénieurs, administrateurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances en systèmes, réseaux et sécurité informatique.

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.

1 Introduction

- Les faiblesses des solutions traditionnelles.
- Pourquoi la messagerie électronique n'est-elle pas sécurisée ?
- Peut-on faire confiance à une authentification basée sur un mot de passe ?
- Usurpation d'identité de l'expéditeur d'un message.

Travaux pratiques

Utilisation des lacunes protocolaires.

2 Cryptographie

- Concepts et vocabulaire.
- Algorithmes de chiffrement symétrique et asymétrique.
- Fonctions de hachage : principe et utilité.
- Les techniques d'échange de clés.
- Installation et configuration d'un serveur SSH.
- SSH et Man in the Middle.
- SSH, l'usage du chiffrement asymétrique sans certificat.

3 Certification numérique

- Présentation du standard X509 et X509v3.
- Autorités de certification.
- La délégation de confiance.
- Signature électronique et authentification.
- Certificats personnels et clés privées.
- Exportation et importation de certificats.

Travaux pratiques

Magasins de certificats Microsoft.

4 L'architecture PKI

- Comment construire une politique de certification ?
- Autorité de certification. Publication des certificats.
- Autorité d'enregistrement (RA).
- Modèles de confiance hiérarchique et distribuée.
- Présentation du protocole LDAP v3.
- Mise en œuvre d'une autorité de certification racine.
- Génération de certificats utilisateurs et serveurs.

Travaux pratiques

Mise en œuvre d'une hiérarchie d'autorités de certification.

5 Gestion des projets PKI : par quelles applications commencer ?

- Les différentes composantes d'un projet PKI.
- Choix des technologies.
- La législation.

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation 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 participant 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

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

6 Panorama des offres du marché

- L'approche Microsoft.
- Les offres commerciales dédiées : Betrusted (ex-Baltimore) et Entrust.
- OpenPKI : la communauté open source.
- IdealX, entre solution commerciale et open source.
- Les offres externalisées Certplus, Versign...

Travaux pratiques

Authentification Web-SSO type SSL v3 avec firewall applicatif.
Authentification forte par certificat X509. Mise en œuvre d'un serveur de messagerie sécurisé et d'un annuaire pour les certificats.

Dates et lieux

CLASSE À DISTANCE
2026 : 24 mars, 2 juin, 15 sep., 15 déc.