Formation PKI, mise en œuvre

Réf : MS555022

OBJECTIFS DE LA FORMATION

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

PROGRAMME

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

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

CERTIFICATION NUMERIQUE
- 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

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 oeuvre d'une autorité de certification racine
- Génération de certificats utilisateurs et serveurs

GESTION DES PROJETS PKI : PAR QUELLES APPLICATIONS COMMENCER
- Les différentes composantes d'un projet PKI
- Choix des technologies
- La législation

PANORAMA DES OFFRES DU MARCHE
- 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...

La formation est accessible aux personnes à mobilité réduite et toute demande d'adaptation peut être étudiée en amont de la formation en fonction du besoin des personnes. Nous contacter pour plus d'informations

Lieu : Site de Metz : JCD FORMATION - 193 rue Metman - 57070 METZ - 03 87 37 97 70
Site de Pompey : KAPEDIA – 132 Rue Léonard de Vinci – 54340 POMPEY – 03 83 49 80 80

3 jours soit 21 h

Voir calendrier

1830 HT / participant

Public / Prérequis

Public
Ingénieurs, administrateurs systèmes et réseaux

Prérequis
Bonnes connaissances en systèmes, réseaux et sécurité informatique..

Méthodes et Moyens pédagogiques

Pédagogie active, avec alternance de phases théoriques et d'exercices pratiques.
Ces derniers permettent une utilisation immédiate et quotidienne des outils proposés.

Salles équipées : vidéoprojecteur, paperboard, ordinateur individuel, support de cours papier ou électronique, outils de prise de note

Validation

Attestation de stage

Profil intervenant

Professionnel et expert en informatique

Suivi et Évaluation de l'action

Compte rendu de fin de formation et analyse interne
Questionnaire « évaluation de la formation » rempli par le stagiaire.

Document mis à jour le 21/07/2022