PKI - mise en oeuvre

3 j (21 heures) Ref : PKII

Public

Expert Système

Pré-requis

Bonnes connaissances en systèmes, réseaux et sécurité informatique

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue - Exposés, cas pratiques, synthèse, assistance post-formation pendant trois mois - Un poste par stagiaire, vidéoprojecteur, support de cours fourni à chaque stagiaire.

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires Questionnaire d'évaluation de la satisfaction en fin de stage Auto-évaluation des acquis de la formation par les stagiaires Attestation de fin de formation

Objectifs

Connaître les éléments structurant une PKI

Mener un projet PKI dans les meilleures conditions

Apprendre à déployer une autorité de certification

Générer des certificats

Mettre en oeuvre une messagerie sécurisée et une solution Single Sign-On (SSO)

Programme détaillé

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

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

Travaux pratiques

Mise en oeuvre d'une hiérarchie d'autorités de certification

GESTION DES PROJETS PKI

Par quelles applications commencer ?