

Sécurisation des données et PKI – Durée : 3 jours Tarif: C

Présentation

Le développement de l'infrastructure réseau intra, extra et internet au sein des entreprises nécessite la mise en place d'une politique de sécurité afin de protéger les données du système d'information et de l'ensemble des communications.

Participants

Ingénieur système, administrateur, responsable sécurité, directeur informatique, chef de projet

Bénéfices

Maîtriser les concepts de clé publique et de certificat

Apprendre à développer l'infrastructure des PKI

Objectifs du cours

Appréhender les enjeux et limites des infrastructures de gestion de clés, d'un point de vue technique comme organisationnel.

Pré-requis

Bonnes connaissances du système d'information.

Programme détaillé du stage : Sécurisation des données et PKI

Module	Points clés
---------------	--------------------

1^{er} Jour: Intrusion : protection et détection

Méthodes d'attaque

- Attaque ciblée et attaque tous azimuts
- Déroulement typique d'une attaque par intrusion
- Différents types d'attaque par saturation (déni de service), Attaques par maliciels

Les outils de protection

- Le pare-feu – différents types de filtrage et autres fonctionnalités
- La sécurité des serveurs, La sécurité des applications
- Les systèmes de détection d'intrusion (IDS)
- Les limites des outils de protection

La sécurité des systèmes d'information

- Analyse de risques: sensibilité et vulnérabilité du système d'information
- Le rôle de l'administrateur, Le rôle du service sécurité

Bases de cryptographie et certificat

Introduction

- Pourquoi ? : Sécurité des communications
- Les protections (DIC, rejeu et non répudiation)
- Les fonctions et mécanismes de sécurité

Les algorithmes et leur utilisation dans les mécanismes de sécurité

- Algorithmes symétriques et asymétriques
- Fonctions de hachage
- Exemple d'authentification en mode symétrique et en mode asymétrique
- La signature électronique

Mise en œuvre des fonctions de sécurité

- Le protocole SSL/TLS
- La messagerie S/MIME

Suite du Programme détaillé du stage : Sécurisation des données et PKI

Module	Points clés
--------	-------------

De la clé publique au certificat

- Nécessité de la certification
- Les certificats X.509
- Champs standards et extension: X509.v3
- Panorama des certificats dans WINDOWS

La problématique de la certification

- Les boîtes à outils
- OpenSSL, PGP

Deuxième Jour: Architecture PKI

- Architecture et composantes
- Entités et rôles
- Structures hiérarchiques et autres
- Génération des clés
- Cycle de vie des certificats, Demande certificat
- Signature de demande de certificat
- Publication de certificat, Révocation de certificat
- Le standard PKCS#11

Annuaire et PKI et les produits disponibles

Annuaire et PKI

- Définition des annuaires et rôles associés
- Le protocole LDAP
- Gestion des certificats dans l'annuaire
- Liste de révocation

Les produits disponibles

- Les offres de produits PKI
- OPENSSL (logiciel libre)
- Les tiers certificateurs (VERISIGN, CERTINOMIS)

3ième Jour – Gestion des projets PKI

- L'organisation de la confiance
- Politique et énoncé de pratiques de certification
- Finalité du projet: sécurité des communications ou signature électronique
- Les différentes composantes d'un projet PKI
- Interlocuteurs concernés
- Choix des technologies
- Mise en œuvre
- Politique sécurité, La législation
- Définition des procédures d'utilisation et d'exploitation

Impact de l'intégration de PKI dans les applications

- Impact organisationnel, Implication juridique
- Intégration au processus métier
- Mesure et conséquence du déploiement
- Mise en place d'une authentification et d'une gestion de connexion SSO