EduGroupe
Accompagner pour réussir

Principes et mise en œuvre des PKI

Référence : **SECPKI** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Formation universitaire de base ou Ingénieur en informatique. • 2-Pas de connaissance de la cryptographie ni des certificats requis. • 3-Utilisation de la ligne de commande, notion d'API bases de réseau IP sont un plus.

PROFIL DES STAGIAIRES

• 1-Architectes. • 2-Chefs de projets. • 3-Responsable sécurité/RSSI avec une orientation technique. • 4-Développeurs séniors. • 5-Administrateurs système et réseau sénior.

OBJECTIFS

• Apprendre les technologies et les normes (initiation à la cryptographie). • Apprendre les différentes architectures. • Apprendre les problématiques d'intégration (organisation d'une PKI, formats de certificats, points d'achoppement). • Apprendre les aspects organisationnels et certifications. • Apprendre les aspects juridiques (signature électronique, clés de recouvrement, utilisation, export / usage international).

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Jour 1 : Mise en contexte

Bases de cryptographie

- Notions de dimensionnement et vocabulaire de base
- Mécanismes
- Combinaisons de mécanismes
- Problèmes de gestion de clés
- Sources de recommandation : ANSSI, ENISA, EuroCrypt, NIST

Implémentation de la cryptographie

- Bibliothèques logicielles
- Formats courants
- Usages courants et gestion associée
- Chiffrement de fichiers et de disques
- Chiffrement de messagerie
- Authentification
- Chiffrement des flux

Grands axes d'attaques et défenses

Exercices OpenSSL d'utilisation des primitives cryptographiques

Cadre général : Historique

Jour 2 : PKI et organisation

Matériel cryptographique

- Différents types d'implémentation matérielle
- Certification Critères Communs
- Certification FIPS 140-2

Structure de PKI

- Certificats X509
- Rôles : sujet, vérificateur, certificateur, enregistrement, révocation o Architectures organisationnelles courantes
- Cinématiques dans PKIX o Hiérarchies d'autorités
- Vérification récursive d'une signature1

Cadre légal et réglementaire

- Droit de la cryptologie
- Droit de la signature électronique
- Référentiel général de sécurité

Certification d'autorité

- ETSI TS-102-042 et TS-101-456, certification RGS
- Exigences pour les inclusions dans les navigateurs et logiciels courants
- Évolution des pratiques
- Exercice : Opération d'une infrastructure de gestion de clés avec Gnomint jusqu'à authentification TLS réciproque

Jour 3 : Implémentation de PKI et perspectives

Suite des exercices de gestion d'IGC et ajout d'une génération de certificat sur token USB

Mise en œuvre de PKI

- Différents types d'implémentation d'IGC rencontrées couramment
- Types d'acteurs du marché
- Recommandations pour l'intégration
- Attaques sur les PKI
- Problème des PKI SSL/TLS
- Remédiations mise en œuvre pour TLS

Infrastructures de gestion de clés non X509

- GPG
- SSH
- R/PKI

Prospective

- Évolution de la cryptographie et modes journalistiques
- Distribution de clés par canal quantique (QKD)
- Cryptographie homomorphique
- Cryptographie-post quantique
- Gestion des clés symétriques
- Chaines de blocs (blockchain)
- Tendances et conclusion