Formation « PKI Windows »

Réf : SECUPKIWIN

Les bases de la cryptographie aux bonnes pratiques organisationnelles, cette formation donne toutes les clés nécessaires à la gestion opérationnelle d'une IGC (PKI) dans un contexte Windows. A travers des cas concrets, les stagiaires apprendront à maîtriser les concepts de base ainsi que le développement de scripts PowerShell afin d'automatiser et de faciliter la gestion de l'IGC (PKI). Une étude de cas regroupant plusieurs cas réels permettra aux stagiaires d'évaluer leur niveau en fin de formation et de se préparer à l'examen.

Objectifs

- Apprendre les technologies et les normes (initiation à la cryptographie)
- Comprendre les besoins métier concernant les certificats
- Acquérir les connaissances et compétences nécessaire afin de fournir un support haut-niveau aux métiers
- Apprendre à créer des scripts Powershell pour gérer et améliorer l'IGC

Durée & horaires

- 3 jours soit 21 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Experts sécurité
- Responsable PKI Windows
- Administrateurs système et réseaux Windows
- Architectes Active Directory

Pré-requis

- Formation universitaire de base ou ingénieur en informatique
- Pas de connaissance de la cryptographie ni des certificats requis
- Connaissance de Windows souhaitable
- Connaissance de powershell pas nécessaire
- Chaque stagiaire doit posséder un compte Microsoft Live afin d'activer une licence temporaire Windows server

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours au format papier en français
- Ordinateur portable avec virtualbox
- Un compte Windows Live (live.com) afin d'obtenir une licence serveur temporaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUPKIWIN par HS2.**

Programme

Cryptographie et PKI

- Rappel sur les principes cryptographiques fondamentaux
- Rappel des algorithmes cryptographiques et taille de clé conseillés
- Architecture organisationnelle et technique d'une IGC (PKI)
- Principe de création, vérification et révocation de certificat
- Création d'une autorité racine indépendante

PKI Windows

- Rappel de l'environnement Windows
- Spécificité de l'IGC (PKI) Windows
- Création d'une autorité fille liée à l'AD
- Rappel des bases Powershell
- Création de scripts simples en Powershell

PKI avancée

- Cas d'étude d'une architecture IGC
- Création de scripts Powershell avancés
- Méthodologie de résolution de problème (debugging)
- Etude de cas : les stagiaires doivent résoudre 6 problèmes utilisateurs dont la difficulté va de moyen à expert
- Examen de certification HS2 (QCM sur ordinateur)