Sécuriser un réseau d’entreprise

Programme *(Mis à jour le 25/05/2022)*

Introduction

- Où sont les risques ?
- D’où viennent les risques
- Pourquoi un risque ?
- Evolution des intrusions
- Taxonomie des menaces
- L’administration de réseau face aux intrusions
- Quelques chiffres

Eléments de cryptographie

- Introduction
- Modélisation des crypto-systèmes
- Cryptographie symétrique (DES, 3DES, AES, RC4)
- Cryptographie asymétrique (RSA, Diffie-Hellman, DSA)
- Les fonctions de hachage (MD5, SHA)
- La signature numérique (Hachage + clé asymétrique)
- Synthèse
- Applications de la cryptographie dans les réseaux

La PKI (Public Key Infrastructure)

- Avantages d’une PKI
- Composants d’une PKI
- Gestion d’une PKI : les contraintes
- Intégration et interopérabilité

Sécurité du système

- La programmation
- Buffer Overflow
- SQL injection
- Failles des systèmes d’exploitation
- Les virus
- Les spywares
- Le pishing
- Le mail : SPAM et HOAX

Méthodes de gestion de l’identité : l’authentification

- Le système AAA
- Le système Kerberos
- Intégration avec les Annuaires
- Les firewalls
- Introduction
- Firewall OS
- Firewall Appliance
- Firewall Personnel
- Le filtrage de paquets
- Principe
- Avantages et inconvénients
- Le filtrage applicatif
- Proxy et Reverse Proxy

Référence

THIS2972

Durée

3 jours / 21 heures

Prix HT / stagiaire

2550€

Objectifs pédagogiques

- Concevoir les vulnérabilités
- Concevoir les principales technologies de sécurisation et les domaines d’application dans la démarche « sécurité de l’entreprise ».

Niveau requis

- Garantir avoir une connaissance de base en réseaux IP

Public concerné

- Responsables sécurité, administrateurs systèmes et réseaux, mais également toute personne impliquée dans l’organisation de la sécurité de son entreprise.

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d’accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N’hésitez pas à nous contacter pour en discuter) équipée d’un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de l'évaluation des résultats de la formation

Feuilles d’émargement (signature électronique privilégiée)
Evaluations formatives et des acquis sous forme de questions orales et/ou écrites (QCM) et/ou mises en situation
Questionnaires de satisfaction (enquête électronique privilégiée)

- Translation d’adresses NAT
- Principe
- Avantages et inconvénients
- Exemples d’architectures Firewall

Les Technologies VPN

- Introduction
- Classification des VPNs
- Les VPNs Ipsec
- Principe
- Principaux protocoles : AH, ESP, IKE
- L’approche L2TP : principe et fonctionnement
- L’approche SSL : principe et fonctionnement
- Synthèse : quelle est la meilleure approche ?
- Exemples d’architectures VPN

Détection et Prévention d’intrusion

- Qu’est ce qu’un IDS/IPS ?
- Qu’est ce qu’une intrusion ?
- Les signatures
- Comment fonctionne un IDS/IPS
- Le Network IDS/IPS
- Le Host IDS/IPS

Conclusion