



Introduction à la sécurité informatique

Objectifs

L'évolution des risques et des technologies dédiée à la **sécurité de l'information** nécessite une vision globale et une approche structurée. Ainsi il est possible d'appréhender les facettes de la sécurité informatique simplement. Cette formation à **vocation non technique** est un premier jalon permettant d'acquérir les bases nécessaires à la compréhension de la sécurité informatique.

Personnels visés

Décideurs, responsables sécurité des systèmes d'information, chefs de projet, responsables informatique, architectes, ingénieurs réseau ou sécurité, directeurs informatique, correspondants sécurité.

Pré-requis nécessaires

Un niveau de **connaissance basique** du Tcp/ip est souhaitable, cependant un module optionnel d'initiation au protocole Tcp/ip permet de suivre cette formation.

Durée

Cette formation est répartie sur **4 jours** :

- | | |
|-----|---|
| 1 | Théorie: introduction, l'intrusion informatique |
| 1/2 | Atelier : l'intrusion informatique |
| 1 | Théorie: solution de sécurisation |
| 1/2 | Atelier : sécuriser son réseau |
| 1 | Validation: QCM, forum et sujets d'actualité. |

Atelier pratique

Méthode d'intrusion réseau et ingénierie sociale. Réalisation et blocage d'une écoute réseau conventionnelle et sans-fil. Usurpation des droits d'un utilisateur, d'un service. Détournement d'un flux switché. Utilisation d'une sonde de détection d'intrusion ...

Vous apprendrez à :

- Visualiser les risques inhérents à votre système d'information,
- Sécuriser les flux d'information de votre réseau,
- Appréhender les principes d'une architecture réseau sécurisée,
- Connaître les menaces informatiques.

Contenu de la formation

Introduction

- Problématique actuelle liée à la sécurité *Humain, technique, stratégique, organisationnel, légal.*
- Définition des besoins en sécurité informatique *CID: confidentialité, intégrité, disponibilité.*
- Évaluation des risques *Définition des risques, formule de calcul,...*
- Détermination des menaces *Méthodologie, erreur, accident, malveillance.*
- Identification des conséquences *Image de marque, crédibilité, coût financier, ...*

L'intrusion informatique

- Module Tcp/Ip (optionnel)
- Identifier le profil de son attaquant *Prestataire, particulier, concurrent, collaborateur.*
- Étudier les moyens utilisés *Méthodologie, type d'outil, schéma d'attaque.*
- Présentation d'une attaque type *Démonstration d'une attaque et analyse.*
- La boîte à outil d'un pirate informatique *Visualiser les outils utilisés par un pirate conventionnel.*
- Attaques réseaux classiques et logicielles *Spoofing, hijacking, man in the middle, ...*
- Attaques d'ingénierie sociale *Définition des moyens, installation d'un relais,...*
- Les vers, virus et bombes logiques *Histoire, Méthode de propagation, techniques, futur.*
- Vision des moyens futurs *Ouverture des médias, les nouveaux P2P, le WiFi, ...*

Solutions de sécurisation

- Gestion des contrôles d'accès et des utilisateurs *Identification, authentification, autorisation, contrôle, ...*
- Surveillance du réseau et méthode monitoring *IDS, audit technique et plan d'actions, test d'intrusion et trophés, ...*
- Sécurité des communications *VPN, NAT, PAT, sécurité du courrier électronique, sécurité téléphoniques, sécurité de la voie.*
- Management de la sécurité *Conduite du changement, classification des données, organisation de la sécurité, politique de sécurité.*
- Architecture sécurisée *Isolation des processus, niveau de sécurité, intégration de la sécurité et vision des « best practices », DMZ.*
- Cryptographie *Histoire, objectifs, chiffrement moderne, application actuelle, attaque conventionnelle.*
- Sécurité des développements logiciels *Méthodologie et contraintes spécifiques.*
- Sécurité de l'exploitation du SI *Antivirus, sauvegardes, supervision.*
- Continuité des activités *PCA, PRA, plan de secours, gestion de crise.*
- Méthodologie d'analyse des risques *Mehari, Ebios, ISO 27001, Cobit, tableaux de bords.*

Droit et conformité réglementaire

- Réglementation générique française *CNIL, DCSSI, signature électronique, chiffrement, courrier électronique, responsabilité pénale.*
- Réglementation spécifique selon l'auditoire *Exemples: Bâle 2, CFR21 Part 11, dématérialisation.*

FREESECURITY
27/29 Rue Raffet
75016 Paris

Tél. 01 46 94 66 53
<http://www.freesecc.net>

FREESECURITYTM

« Des experts au service de votre sécurité »