La sécurité informatique : systèmes et réseaux

Public concerné par la formation : Les informaticiens souhaitant acquérir des notions avancées sur la sécurité informatique au sein de leur entreprise

Pré-requis : Connaitre les protocoles réseaux

Objectifs à atteindre :

- ✓ Comprendre et savoir mettre en œuvre la sécurité informatique au sein de l'entreprise.

Moyens pédagogiques, techniques et encadrement : Formateur permanent, poste de travail individualisé, vidéo projecteur, support de cours.

Durée de la formation : La durée de la formation varie en fonction du niveau de base de l'apprenant. Le plan de formation est divisible en trois niveaux: Initiation, Perfectionnement et Expertise

TCP/IP

- ✓ Les protocoles TCP/IP
- ✓ Les forces et les faiblesses du protocole TCP/IP

Etat des lieux

- ✓ Quels sont les enjeux de la sécurité ?
- ✓ Quels sont les risques ?
- ✓ Identifier les critères de sécurité
- ✓ Quelles sont les normes liées à la sécurité ?

Identifier les vulnérabilités des postes utilisateurs

- ✓ Les intrusions à distance : navigation Web, clients de messagerie…
- ✓ Les chevaux de Troie…

Identifier les vulnérabilités du réseau

- ✓ Attaques des règles de Firewalling, interception/analyse des transmissions réseaux cryptées
- ✓ Sniffing réseau
- ✓ Spoofing réseau / Bypassing de firewall
- ✓ Idle Host Scanning
- ✓ Détournement de connexions
- ✓ Attaque des protocoles sécurisés
- ✓ Dénis de service

Identifier les vulnérabilités du web

- ✓ Attaque des scripts Web dynamiques (PHP, Perf…), et des bases de données associées (MySql, Oracle…)
- ✓ Cartographie du site
- ✓ Failles PHP (include, fopn…)
- ✓ Attaques CGI (Escape shell…)
- ✓ Injections SQL
- ✓ XSS

Identifier les vulnérabilités applicatives

- ✓ Intrusion à distance d'un système Windows et Linux par l'exploitation des services de type applicatif, avec la plateforme Metasploit
- ✓ Escape shell
- ✓ Buffer overflow

Mise en pratique

La sécurité des échanges de données

- ✓ Quelles sont les contraintes de sécurité ? (intégrité, confidentialité…)
- ✓ Quels sont les différents principes de chiffrement ?
- ✓ Quelles sont les contraintes liées au support ? (espionnage…)

Sécurisation de Linux

- ✓ Permissions standards et étendues
- ✓ Gestion des profils de sécurité et des
- ✓ Limitations des applications
- ✓ Utilisation de PAM

- ✓ Mise en place du pare-feu sur Linux
- ✓ Manipulation du chiffrement disque sur Linux
- ✓ Gestion des intrusions et des journaux (logs)

Sécurisation de Windows

- ✓ Gestion des droits
- ✓ Gestion des services
- ✓ Accès problématiques pour le réseau et les périphériques
- ✓ Configuration du pare-feu, et réflexions
- ✓ Possibilités de chiffrement
- ✓ Gestion du journal d'évènement et des audits

Audit d'un système

- ✓ Analyse externe au niveau réseau
- ✓ Inventaire des risques opérationnels
- ✓ Vérification du cloisonnement applicatif et utilisateur
- ✓ Risques liés à la maintenance du système (versions des logiciels, mauvaises configurations)
- ✓ Tentatives d'intrusion ciblées

Méthodes pédagogiques : Alternance entre apports théoriques et mises en applications directes sur des exemples académiques ou issus de l'environnement professionnel des stagiaires

Evaluation des acquis : Réalisation individuelle, au cours de la formation, d'exercices de validation des compétences acquises.
Mise en place, en fin de module, d'un exercice récapitulant l'ensemble des fonctionnalités vues en formation.
Feuille d'émargement journalière et bilan écrit à chaud.