Sécurité Systèmes et Réseaux
Notions fondamentales

2 jours
soit 14 heures

Réf : ssr2

Objectifs

A la fin de la session, le stagiaire doit être capable de mettre en œuvre les principaux moyens de sécurisation des systèmes et des réseaux Internet/Intranet (architecture, firewall, mise en œuvre).

Public

Responsable sécurité. Ingénieur système et réseaux. Architecte sécurité. Techniciens réseaux ou sécurité. Administrateurs réseaux.

Niveau requis

Bonne connaissance du protocole TCP/IP, du routage, de l'administration système et réseaux sous Linux et Windows 2000. Quelques connaissances sur les réseaux WiFi seraient un plus

Pédagogie

- Apports théoriques étayés par de nombreux exercices pratiques
- Console individuelle
- Contrôle permanent des acquis
- Support de cours
- Evaluation par questionnaire en ligne en fin de stage
- Attestation de fin de stage
- Assistance post-formation
- Formateur intervenant professionnel et expérimenté maîtrisant les techniques professionnelles

Risques et menaces

- La sécurité dans le monde TCP/IP (Etat des lieux de la sécurité informatique, vocabulaire sécurité)
- Attaques en mode noyau (Forces et faiblesses du protocole TCP/IP, IP Spoofing, TCP-flooding, SMURF, déni de service.)
- Attaques applicatives (récupérer les informations publiques de votre entreprise, les applications à risque (DNS, HTTP, SMTP, etc.). Spamming et « relais noir ».)

Architectures de sécurité

- Quelles architectures pour quels besoins ? (Routeur filtrant, firewall, DMZ., plan d'adressage sécurisé, translation d'adresses NAT/PAT/MASQ/STATIC)
- Firewall (Dédier un firewall ou le mutualiser ?, architectures multi-niveaux, points de filtrage, critères de choix et mode d'implémentation, les étapes de la méthodologie de projet firewall..)
- Proxy serveur et relais applicatif (Proxy ou firewall, reverse proxy, filtrage de contenu, cache et authentification. relais SMTP)

Sécurité des réseaux TCP/IP

- Sécuriser les accès réseaux WAN (Auditer et renforcer, méthode et application, fonctions du Firewall, réseaux privés virtuels)
- Sécurité WiFi (Risques, WEP, WPA, architectures de déploiement, norme 802.11i/WPA2.)
- Disponibilité et qualité (QoS , les outils, logiciel dédié, réseaux privés virtuels.)

Sécurité des bastions

- Durcissement des bastions Windows (Correction des failles, les étapes du renforcement de la sécurité Windows, sécurité applicative)
- Durcissement des bastions Linux Debian (La règle du « toujours trop » sur Linux, les étapes du renforcement de la sécurité sous Linux, sécurité applicative)

Sécurité des données

- Public Key Infrastructure (les chiffrements symétrique et asymétrique, fonctions de hachage, certificat et signature électronique, certificats révoqués)
- Authentification de l'utilisateur (Techniques d'authentification, l'authentification forte, certificats, Radius, LDAP)
- Vers, virus, trojans, malwares et keyloggers (Tendances, organiser sa défense, outils et méthodes.)

Audit sécurité et exploitation

- Définir et conserver un seuil de sécurité (Mesurer la sécurité, cycle de vie d'une faille, la lutte contre le temps)
- Les outils et techniques disponibles (Tests vulnérabilité intrusion : outils et moyens, logiciels de scan avancé Scanner, Nessus, outils de détection temps réel IDS-IPS, agent, sonde ou coupure.)
- Réagir efficacement en toutes circonstances (procédures de réaction, veille technologique des nouvelles vulnérabilités)