G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

Sécurité Wi-Fi

But de la formation

Acquérir la compréhension globale du fonctionnement d'un réseau Wi-Fi, en appréhender les risques et les méthodes de sécurisation.

Pré-requis

Aucun prérequis défini

Type de public

Ce cours s'adresse aux responsables de sécurité, aux responsables informatique, réseaux et télécoms, aux consultants, ainsi qu'aux administrateurs réseaux et sécurité, afin de leur permettre de mettre en oeuvre des solutions de sécurité sur leur réseau Wi-Fi.
Ce cours sera également utile aux chefs de projets souhaitant utiliser des technologies de réseaux sans fil.

La connaissance préalable des réseaux et des protocoles TCP/IP sont recommandée ; des rappels sont toutefois effectués en début de cours.

Méthodes pédagogiques

Cours magistral, avec exemples pratiques et exercices illustrant les différentes attaques décrites en cours.
TP final permettant la mise en oeuvre d'une architecture sécurisée.

Durée

14 heures (2 jours).

Programme

- Généralités sur les réseaux sans fils
  - Technologies
  - Normes
  - Matériel (composants)
  - Problématiques liées à la sécurité
    - Propriétés du média
    - Déni de service
- 802.11 - Principes
  - Canaux et fréquences
  - Eléments d'architecture
  - Services
  - Trames
- Caractéristiques de la technologie
  - Physique
  - Antennes et environnement
  - Portée des réseaux sans-fil
  - Positionnement dans l'architecture

- Attaques sur la technologie Wi-Fi - Généralités
    - Attaque sur le 802.11
    - Brouillage
        - Exemple de brouillage
    - Usurpation de borne
    - Inondation de messages
    - Wi-Fishing
    - Audit et outils
        - Scanners (actifs / passifs)
            - Cas pratique d'utilisation basique
        - Aircrack
            - Cas pratique d'utilisation basique
    - Matériel (antenne, station, etc.)
- WEP
    - Principe
    - Faiblesses et vulnérabilités
    - Attaques
        - Cas pratique : cassage de clé WEP
- 802.1X
    - Introduction
    - Principe
    - Chiffrement
    - Authentification
    - Radius
    - EAP, TLS, PEAP, etc.
- WPA/WPA2
    - Principe
    - Différentes normes et configurations
    - Faiblesses
    - Attaques
        - Cas pratique : cassage WPA/WPA2 personnel (PSK), attaques TKIP
- Gestion des réseaux Wi-Fi
    - Gérer ses réseaux Wi-Fi
        - Acteurs et rôles
    - La sécurité intrisèque des bornes
    - Architecturer correctement ses réseaux Wi-Fi
    - Authentifier les utilisateurs de WLAN
- Mise en place d'une architecture Wi-Fi sécurisée
    - Problématiques
    - Exemples d'architectures
    - Préconisations
        - PEAP/MSCHAPv2 - EAP/TLS
        - Cloisonnement
        - Configuration des postes clients
        - Configuration centralisée des équipements
    - Cas pratique final