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

Programme de formation

Sécurité des réseaux sans fil

But de la formation

- Les atouts et faiblesses des principales technologies sans-fil
- Comment utiliser les technologies sans fil en toute sécurité
- Auditer vos propres installations

Pré-requis

- Avoir une expérience dans l'utilisation des systèmes Windows et Unix/Linux
- Avoir de bonnes connaissances des principaux protocoles TCP/IP

Type de public

- Experts en sécurité de l'information
- Consultants
- Auditeurs
- Administrateurs systèmes et réseaux

Moyens pédagogiques

- Ordinateurs portables mis à disposition du stagiaire
- Supports en français

Sanction de la formation

- Cette formation n'est pas certifiante.
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral
- Travaux pratiques

Durée

14 heures (2 jours).

Programme

Généralités sur les réseaux sans-fil

- Panorama des technologies et des normes
- 802.XX
    - Bluetooth
    - Wi-Fi
    - Zigbee
    - WiMAX
- Filtrage
- Infrarouge
- NFC
- GSM / UMTS / LTE
- TETRA

Caractéristiques des technologies

- Problématiques physiques
- Brouillage radio
- Environnement (absorption, diffraction, réfraction, réflexion / humidité, verre, béton, etc...)
- Écoutes et interceptions
- Détournement de connexion
- Insertion et rejeux de trafic
- Risques sanitaires
- Méthodes de transmission
- FHSS
- DSSS
- IR
- DSSS/CK
- OFDM
- Études, démonstrations et cas praques d'attaque sur le 802.11 CSMA/CA

- Utilisation abusive du média (réservation du temps)
- Saturation radio
- Envoi de trames de désassociation
- Déni de service sur la batterie

Technologie Wi-Fi

- Répartition du spectre 2,4GHz
- Positionnement dans l'architecture du SI
- Présentation des attaques sur le 802.11
- Usurpation de borne / client
- Désassociation / Désauthentification
- Vol de paquets en attente
- Wi-Fishing
- Écoute passive
- Présentation d'outils logiciels (Kismet, aircrack-ng, etc...)
- Présentation d'outils matériels (WiFi Pineapple, BVS, etc...)
- Sécurités
- WEP
- 802.1X (EAPoL, RADIUS, PEAP, MSCHAPv2, etc...)
- WPA / WPA2
- WPS
- Exemple et étude d'une architecture sécurisée
- Pour chaque partie, démonstrations et cas pratiques d'attaques :
- Mise en place et configuration de la sécurité proposée
- Attaques sur la solution
- Études des améliorations possibles

SDR

- Sécurités
- Présentation
- Récepteur et antennes
- GNU Radio Companion
- Démonstrations avec la HackRF

Bluetooth

- Technologies (classique, BLE, etc...)
- Sécurité et faiblesses
- Présentation d'outils d'analyse et d'attaques (BTScanner, Redfang, BtleJuice, etc...)
- Présentation d'outils physiques (Ubertooth One, Bluefruit LE Sniffer)
- Attaques
- Reconnaissance
- Spam
- Vol d'informations
- Contrôle à distance
- Attaques sur la crypto
- Dénis de service
- Highjacking / Spoofing
- Attaques sur les mauvaises implémentations

Zigbee

- Présentation des technologies
- Sécurité et faiblesses
- Études des attaques existantes

NFC

- Présentation des technologies (Mifare / DESFire / etc...)
- Sécurité et faiblesses
- Études des attaques existantes (lecture d'informations, copie, rejeu, etc.

- Cas pratique de lecture et copie d'une carte NFC
- Proposition et étude d'une architecture sécurisée

Téléphonie mobile

- Panorama des technologies
- GSM / 2G
- Présentation de la technologie
- Extensions (2G+, 2,75G)
- Fonctionnement du Short Message Service (SMS - RFC 5724)
- Sécurités et faiblesses sur les méthodes de chiffrements (A5/1, A5/2, A5/3)
- Attaque par régression du protocole
- UMTS / 3G
- Présentation de la technologie
- Extensions (3G+, H+)
- Sécurités et faiblesses
- LTE / 4G
- Présentation de la technologie
- Extension (4G+)
- Sécurités et faiblesses

TETRA

- Présentation de la technologie
- Comparaison avec le GSM
- Sécurité et faiblesses
- Études d'attaques existantes (écoute, rejeu)
- Démonstration d'une écoute de communication