Formation « Sécurité et Red Team Wi-Fi moderne »

Réf : SECUWIFI

Objectifs

- Comprendre la sécurité Wi-Fi dans sa globalité
- Apprendre à attaquer, à détecter et à défendre un réseau Wifi
- Identifier les points faibles et erreurs courantes sur les architectures existantes

Durée & horaires

- 2 jours soit 14 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Toute personne intéressée par la compréhension de la sécurité Wi-Fi dans sa globalité.

Pré-requis

- Connaissances de base en Linux (lignes de commande, compilation, etc.)
- Base en réseaux et manipulation d'outils de visualisation tels que Wireshark, Scapy est un plus
- Connaissances en sécurité offensive ou défensive
- Des connaissances en Wi-Fi sont un plus

Méthode pédagogique

- Cours magistral avec échanges interactifs
- Travaux pratiques

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- Cette formation n'est pas certifiante.

Programme

1. IEEE 802.11

2. Réseaux sans-fil
- Les différents modes
- Sécurité actuelle suivant les modes

3. Choix du matériel
- Cartes d'acquisition
- Antenne
- Optimisation de la transmission
- Amplificateurs et connecteurs
- Problèmes courants

4. Linux et module noyaux
- Introduction
- Pile protocolaire et modules
- Différences SoftMAC et HardMAC
- Chargement de module
- Problèmes courants

5. Inspection réseau
- Monitoring et identification de réseaux
- Analyse de paquets
- Manipulation de paquets
- Interactions avec un point d'accès
- Analyse de « probe requests »

6. Attaques
- Modes:
  - Réseaux ouverts
  - WEP – WPA/WPA2
  - WPA/WPA2 entreprise – WPS
  - WPA3
- Relais
- Vulnérabilités publiques
- Méthodes Red Team et retour d'expérience
- Procédures d'attaques adaptées aux conditions
- etc.

7. Aller plus loin
- Recherche de vulnérabilités
- Attaque de la pile protocolaire
- Débogage avec Nexmon
- Outillage discret et minimalisation
- etc.

Dates de nos prochaines sessions disponibles sur la page :
https://www.hs2.fr/secuwifi