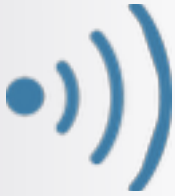
Formation Sécurité des systèmes Wireless

Objectif :

Effectuer des tests de sécurité sur le matériel sans fil

Prérequis :

notions de réseau, de systèmes d'exploitation, de programmation, de théorie des ondes.



Jour 1 : Bluetooth

- Historique
- Normes
- Les services et protocoles
- Les profils d'application
- L'appairage
- Les équipement bluetooth
- Structure matériel
- Protocoles et structure logiciel
- Risques classiques
- Risques spécifiques
- Les outils matériels et logiciels
- Les contre-mesures
- Protocoles et structure logiciel
- Risques classiques
- Risques spécifiques
- Les outils matériels et logiciels
- Les contre-mesures

Jour 2 : RFID

- Définition de la technologie RFID
- Historique
- Les systèmes utilisant la technologie RFID
- Les différentes technologies RFID
  - 125 Khz, 13,56 Mhz
  - Mifare classic (les plus répendues)
  - techniques de transmission des données et alimentation
- Caractéristiques des Tags et badges
  - pécificités (mémoires ...)
  - structure interne (secteurs, blocks, UID ...)
- Les faiblesses
  - système de chiffrement (crypto1)
  - recopie de Tag
  - modification de l'UID (carte chinoise)
- Les outils de hacking
- Tests pratiques et démonstration
- Les contre-mesures

Jour 3 : Domotique

- Définition de la domotique
- Les systèmes appartenant à la domotique
- Les points d'entrée pour le hacking
  - réseau filaire (éthernet)
  - WIFI
  - les bus filaires domotiques
  - les télécommandes radio fréquence
- Les codes utilisés dans les radios commandes
  - codes fixes
  - codes à décalage
  - codes tournants
  - les trames de base
- Rappels sur la radio transmission
  - ondes électromagnétique
  - émetteurs récepteurs
  - les antennes
  - fréquence porteuse
  - la modulation (AM, FM, OO-ASK, OO-FSK…)
- Investigation et paramètres essentiels
  - recherche de la fréquence porteuse
  - recherche du type de modulation
  - type de codage
- Équipement disponible pour le hacking
  - analyseur de spectre
  - clé RTL – SDR
  - USRP
  - HackRF

Jour 4 : Domotique

- Rappels sur la radio transmission
  - ondes électromagnétique
  - émetteurs récepteurs
  - les antennes
  - fréquence porteuse
  - la modulation (AM, FM, OO-ASK, OO-FSK…)
- Investigation et paramètres essentiels
  - recherche de la fréquence porteuse
  - recherche du type de modulation
  - type de codage
- Équipement disponible pour le hacking
  - analyseur de spectre
  - clé RTL – SDR
  - USRP
  - HackRF
- Fonctionnement de GNU Radio
  - présentation
  - la conversion directe
  - les signaux IQ
  - quelques bases mathématiques
  - réalisation de diagrammes GNU Radio compagnon
    - traitement de base de signaux
    - filtrage
    - démodulation

48, Avenue Bellefontaine

59250 Halluin

(+33) 03.66.72.48.44

Pour vous inscrire, merci de nous communiquer vos besoins, identités, financements et dates par courriel :

formations@serval-concept.com