

Bluetooth et WiFi

Objectifs

- ▶ Évaluer objectivement les risques pesant sur les technologies sans-fil WiFi et Bluetooth
- ▶ Mettre en pratique les attaques les plus connues, telle que la cryptanalyse de WEP
- ▶ Connaître les points essentiels pour sécuriser un service WiFi

Des travaux pratiques seront effectués tout au long de la formation (utilisation d'outils).

Durée : 3 jours

Code : BWI

Pré-requis

- ▶ Connaissance du fonctionnement des systèmes d'exploitation
- ▶ Connaissance du fonctionnement des réseaux
- ▶ Connaissance minimale (capacité à relire un code) des langages C, PERL, Python

Prix : 2 400 € HT

Contenu

- ▶ Bluetooth
- ▶ WiFi

Programme détaillé au dos.

Catalogue :

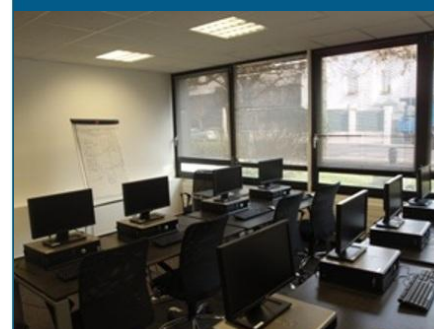
www.atlab.fr/formations.html

Inscription :

contact@atlab.fr
Tél : 01 47 08 88 00

Informations pratiques

- ▶ Participants : un maximum de 10 inscrits
- ▶ Formateur : expert sécurité/R&D
- ▶ Matériel : poste individuel, mêmes systèmes et outils que le formateur
- ▶ Locaux : 75 avenue Victor Hugo 92 500 Rueil-Malmaison
5 minutes à pieds du RER Rueil-Malmaison (sortie 5 Victor Hugo)
(Parking disponible sur simple demande)



Jour 1 : Bluetooth

Présentation de la norme

Historique des attaques

BlueSnarf
BlueBug
BlueSmack
Autres attaques

Attaques bas niveau : mythe ou réalité ?

Attaque des drivers
Attaque des piles
Attaque radio
Etat de la cryptanalyse des protocoles Bluetooth

Outils gratuits disponibles

Jour 2 : WiFi

Présentation des normes 802.11 de A à Z

Faiblesses congénitales du WiFi

Brouillage radio
Désassociation
Faux AP

Sécurité de WEP

Principes
Injection de paquets : "chop chop"
Attaque statistique : "aircrack"

Travaux pratiques : cassage d'une clé WEP-128

Sécurité de WPA/WPA2

Travaux pratiques : cassage de WPA-PSK par dictionnaire

Jour 3 : WiFi suite

Attaques des drivers

Travaux pratiques : exploitation d'une faille dans un driver WiFi

Attaques des implémentations

Stockage des clés sur le client
Politiques d'association

Travaux pratiques : attaque d'un client Windows par un vrai-faux AP

Attaques des AP

Travaux pratiques : intrusion sur un point d'accès

Architectures de sécurité

L'isolation inter-clients : principes
L'isolation inter-clients : failles
Le portail captif : principes
Le portail captif : failles
Authentification 802.1x
Revue des autres protocoles d'authentification

Travaux pratiques :

Établissements de tunnels ICMP et DNS à travers un portail et vol d'une session client sur un portail captif

Exemples d'implémentations réelles

Outils gratuits disponibles