+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 26/07/2023

S'inscrire

# Formation Reconversion Sécurité des Systèmes embarqués et IoT

5 jours (35 heures)

## PRÉSENTATION

Avec l'essor de l'usage des objets connectés, la protection envers l'internet des objets (IoT) est essentielle. Pouvoir se protéger contre les attaques visant les objets connectés vous permettra de protéger les données de vos clients ainsi que gagner un avantage concurrentiel certain.

Après avoir suivi cette formation complète de 5 jours, vous pourrez vous reconvertir en professionnel de sécurité IoT et systèmes embarqués. Ce cours vous enseignera les différents types d'attaques et comment s'en prémunir, l'architecture des systèmes embarqués, l'hardware hacking, l'accès au logiciel et les différentes méthodes de protection.

Cette formation reconversion sécurité des systèmes embarqués et IoT contiendra de nombreux exercices pratiques basés sur des scénarii d'attaque/défense. Ces travaux pratiques, amélioreront votre capacité d'exécution en situation réelle.

## OBJECTIFS

- Connaître les méthodes pour réaliser des audits de sécurité hardware
- Être en capacité de réagir face à une attaque visant des IoTs ou les systèmes embarqués

## PUBLIC VISÉ

- Professionnels de la sécurité IT
- Personnes intéressées par les aspects de sécurité liés au hardware ou à l’embarqué
- Amateurs ou professionnels en électronique

## Pré-requis

- La maîtrise de Linux en ligne de commande est un plus
- Administration Windows/Linux

# PROGRAMME DE NOTRE FORMATION RECONVERSION SÉCURITÉ DES SYSTÈMES EMBARQUÉS ET IOT

## Fondamentaux

- Les particularité des systèmes embarqués
- Les architectures des différents systèmes
- Les inconvénients liés à l'utilisation des systèmes embarqués

## Les cyberattaques

- Les différents types d'attaques
- Les acteurs de la cybersécurité
- Analyse et tests d'intrusion

## Présentation de l'embarqué et de l'IoT

- Système d'exploitation embarqués : Win, Linux ou Raspbian
- Les différents réseaux (LTE, WiFi, 4G, LoRA...)
- Présentation des différents composants (puce, JTAG, UART, caméra...)
- Cryptographie
- Architecture (ARM, MIPS, SuperH)
- TP: Découvrir les cartes Arduino et Raspberry

## Vulnérabilités des architectures embarquées

- Les vulnérabilités les plus importantes
- Recherche de vulnérabilités
- Différentes métodes d'authentification
- Connectivité : réseau, capteur et périphérique
- La méthodologie pour réaliser des tests d’intrusion
- Analyseurs
- Débog
- Désass et Décompil
- TP: Niveau de sécurité d'une architecture embarquée

## Introduction au Hardware Hacking

- Présentation des attaques sur les objets connectés
- Présentation des vulnérabilités
- Introduction à l'électonique

- TP : Prise d’information sur la cible (fingerprint des composants)

### L'intrusion au hardware

- Méthode pour auditer un produit
- Plan d’audit et différences avec l’audit logiciel
- TP : Extraire des données sensibles avec Hardsploit
- TP : Acquérir les signaux électroniques, outils et démonstration

### Accéder au logiciel

- Architecture Microcontrôleur, FPGA
- Interfaces E/S (I2C, JTAG / SWD, SPI...)
- Attaques à canal latéral
- TP : Accès au Firmware par différentes interfaces

### Attaques sur l’objet connecté

### Sécuriser son matériel

- Cycle SDLC
- Bonnes pratiques de sécurité
- Limiter les accès JTAG
- Les vulnérabilités au niveau de l’embarqué
- Se protéger contre les attaques à canal latéral

### SDR Hacking

- Mettre en place un audit SDR
- Présentation des outils (GNURadio, etc.)
- TP : Rétro-ingénierie d’un protocole sans fil

### Exercice « Capture The Drone or the Car»

- Scénario d'Attaque-Défense d’un mini-drone ou d’une voiture connectée

## Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

## Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

## Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

## Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

## Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.