MAJ 16/01/2025

Formation « Sécurité des dispositifs IoT »

Réf : PENTESTOBJ

La montée en puissance des dispositifs IoT (Internet des Objets) dans de nombreux secteurs tels que l'industrie, l'automobile, le médical a multiplié les surfaces d'attaque potentielles. Cette formation vous permettra de vous mettre dans la peau d'un attaquant afin de comprendre, analyser et sécuriser les dispositifs IoT contre les cyberattaques. Elle est conçue pour les professionnels de la sécurité souhaitant approfondir leurs connaissances en matière de tests d'intrusion sur des systèmes IOT.

Objectifs

L'objectif principal de cette formation est d'acquérir les compétences nécessaires pour évaluer et renforcer la sécurité des dispositifs IoT. Les participants apprendront à :

- **Se mettre à la place d'un attaquant pour identifier les vulnérabilités potentielles.**
- **Utiliser des outils et techniques spécifiques pour évaluer la sécurité des dispositifs IoT.**
- **Mettre en place des stratégies efficaces pour défendre ces dispositifs contre les attaques.**

Durée & horaires

- **5 jours soit 35 heures**
- **Horaires : de 9h30 à 12h et de 13h30 à 18h00.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Pentesters**
- **Développeurs**
- **Électroniciens**

Pré-requis

- **Avoir une expérience préalable dans l'un des domaines suivants : tests d'intrusion, développement logiciel, ou électronique, en particulier dans le contexte des dispositifs IoT.**
- **Connaissances de base en reverse engineering et sécurité informatique.**

Méthode pédagogique

- **Cours magistral avec travaux pratiques et échanges interactifs**
- **Les concepts essentiels développés dans la formation sont illustrés au travers de mises en pratique permettant d'acquérir des compétences concrètes applicables en sécurité des dispositifs IoT.**
- **Un réseau vulnérable et des dispositifs IoT sont utilisés pour les tests et les exercices pratiques.**

Supports

- **Support de cours numérique en Français projeté**
- **Support de cours en Français imprimé en mode présentiel, au format numérique en mode distanciel**
- **Cahier d'exercices**
- **Cahier de corrections**
- **Ordinateur portable prêté pour la réalisation des exercices**

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**
- **Evaluation de pré-formation envoyée avant le début de la formation**
- **Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques**

- **Examen final à la fin de la formation (cf certification)**

Ces évaluations ont pour but de valider les compétences acquises.

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTESTOBJ par HS2.**

Programme

Jour 1

1. Introduction Générale à l'IoT :

- Présentation des concepts de base de l'Internet des objets (IoT).
- Démarche d'analyse globale.

2. Retour d'Expérience sur les Stratégies d'Attaque et de Défense :

- Partage d'expériences pratiques sur les différentes stratégies d'attaque et de défense dans le domaine de l'IoT.

Jour 2

3. Reverse Engineering Hardware :

- Présentation et utilisation des outils couramment utilisés par les attaquants.
- Identification et observation des ports de communication intéressants (I2C/UART).
- Travaux Pratiques :
  - Identification des composants clés.
  - Sniffing I2C/UART.
  - Timing Attack.
  - Conception d'un sniffer à base de FPGA (ice40 + Migen/Misoc).

4. Récupérer et Analyser le Firmware :

- Identification du port JTAG
- Familiarisation avec les outils et processus d'extraction
- Structure d'un firmware
- Travaux Pratiques :
  - Bruteforce JTAG.
  - Extraction SWD.

Jour 3

5.Reverse Software :

- Notions d'ASM ARM
- Présentation des outils d'analyse statique
- Sécurité applicative et objet connecté
- Travaux Pratiques :
  - Simple coding ASM.
  - Ghidra / R2 : prise en main de l'outil.
  - Stratégies d'analyse / Recherche de bugs.
  - Chargement de FW.
  - SVDLoader + Ghidra.
  - Password + XOR sur USB.
  - Overflow classique sur UART.
  - Introduction à GDB pour le reverse.
  - Déboggage des binaires pour obtenir des informations sensibles.

Jour 4

6. Attaques par Faute :

- Les attaques par faute

- Cas d'usages
- Méthodes d'exploitation
- Travaux Pratiques :
  - Utilisation du Chipwhisperer sur STM32.
  - Conception d'un outil de glitch simple à base de FPGA (ice40 + Migen/Misoc).
  - Glitch compteur
  - Contournement des restrictions JTAG.
  - Bypass RDP sur STM32.

Jour 5

7. Introduction à la Radio IoT (WiFi, Bluetooth/BLE) :

- Introduction aux protocoles sans-fils
- Introduction aux concepts de traitement du signal logiciel
- Présentation du Bluetooth
- Outils et méthodes d'attaques

- Travaux Pratiques : Concepts de base sur les communications radio dans les dispositifs IoT.
  - Captures de communications (Radio, Bluetooth, etc.).
  - - Analyse des protocoles cryptographiques.
  - - Analyse des interactions avec des composants externes.

Références

- [ISO/SAE 21434](https://www.isit.fr/fr/article/iso-sae-21434.php)
- [Recommandations relatives à la sécurité des systèmes d'objets connectés](https://cyber.gouv.fr/publications/recommandations-relatives-la-securite-des-systemes-dobjets-connectes)
- [ETSI EN 303 645 V2.1.1](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf)