DOCAPOSTE Institute

Formation Test d'intrusion des objets connectés IOT

Présentation

Cette formation en sécurité des objets connectés couvre l'écosystème IoT, la reconnaissance et la cartographie des systèmes IoT, l'analyse matérielle et du firmware, ainsi que les attaques sur les protocoles et réseaux IoT. Les participants apprendront également à sécuriser les interfaces web et mobiles, et à mettre en œuvre des contre-mesures pour protéger les objets connectés.

Durée : 21,00 heures (3 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

- Identifier les menaces spécifiques et les réglementations en vigueur.
- Utiliser des outils pour cartographier et analyser les dispositifs IoT.
- Effectuer du reverse engineering et analyser les firmwares.
- Mettre en œuvre des attaques et des contre-mesures efficaces.
- Tester et renforcer la sécurité des applications et des services cloud associés.
- Identifier les vulnérabilités et proposer des recommandations de sécurité.

Prérequis

- Une compréhension des concepts fondamentaux en informatique et en réseaux est essentielle.
- Avoir des bases en programmation (Python, C, ou C++) peut être très utile, surtout pour l'analyse de firmware et le reverse engineering.
- Avoir un bon esprit d'analyse pour comprendre et identifier les vulnérabilités dans les systèmes IoT.

Public

Cette formation s'adresse aux professionnels de l'informatique souhaitant renforcer leurs compétences en sécurité IoT, aux étudiants et chercheurs en informatique ou cybersécurité, aux développeurs et ingénieurs concevant des solutions IoT, ainsi qu'aux décideurs et gestionnaires responsables de la sécurité des objets connectés dans leur organisation.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

DOCAPOSTE Institute

Programme de la formation

1/ Introduction à la Sécurité des Objets Connectés

- Définition et écosystème de l'IoT
- Architecture d'un système IoT : appareils, passerelles, cloud, applications mobiles
- Enjeux et menaces spécifiques à l'IoT
- Réglementations et normes en cybersécurité IoT (ISO 27001, IoT Security Foundation, GDPR, NIST)

2/ Reconnaissance et Cartographie des Systèmes IoT

- Identification des dispositifs IoT et cartographie du réseau
- Analyse des protocoles de communication IoT (MQTT, CoAP, Zigbee, LoRa, BLE, etc.)
- OSINT et collecte d'informations (Shodan, Censys, IoT search engines)
- Analyse des métadonnées et des configurations exposées

3/ Analyse Matérielle des Objets Connectés

- Démontage et reverse engineering du hardware
- Identification des ports de communication (UART, JTAG, SPI, I2C)
- Dumping et analyse de la mémoire flash (firmware extraction)
- Interception et manipulation des signaux radio (SDR, RFID, NFC)

4/ Analyse du Firmware et Exploitation des Vulnérabilités

- Techniques d'extraction du firmware (JTAG, SPI, NAND, UART)
- Analyse statique et dynamique du firmware
- Détection des vulnérabilités logicielles (buffer overflow, injections, failles crypto)
- Automatisation de l'analyse avec Binwalk, Radare2, Ghidra, Firmware Mod Kit

5/ Attaques sur les Protocoles et Réseaux IoT

- Sniffing et interception des communications réseau

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Analyse et exploitation des failles des protocoles IoT (Zigbee, Bluetooth, MQTT, LoRaWAN)
- Attaques MITM (Man-in-the-Middle) sur les objets connectés
- Détection et exploitation des vulnérabilités Wi-Fi (WPA2, KRACK, Evil Twin)

6/ Sécurité des Interfaces Web et Mobile liées à l'IoT

- Tests d'intrusion sur les applications mobiles IoT (Android/iOS)
- Reverse engineering des APK et identification des failles (Frida, JADX, MobSF)
- Sécurité des API IoT (REST, WebSockets, GraphQL)
- Attaques sur les services Cloud liés aux objets connectés

7/ Exploitation et Contre-Mesures

- Prise de contrôle d'un objet connecté à distance
- Attaques par déni de service (DDoS, botnets IoT - Mirai, Mozi)
- Bonnes pratiques de sécurisation des objets connectés
- Implémentation de mesures de défense : chiffrement, authentification, segmentation réseau

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France