Date de publication : 23/08/2024

Formation : Hacking et Pentest : IoT

Formation pratique - 3j - 21h00 - Réf. HIO
Prix : 2470 CHF H.T.

4,2 / 5

L'internet des objets (IoT) est en pleine évolution et se mêle désormais à notre vie quotidienne, c'est pourquoi ils sont un des grands enjeux de la sécurité informatique. Il faut connaitre leurs failles pour pouvoir déclencher la riposte appropriée et en élever le niveau de sécurité.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Définir l'impact et la portée d'une vulnérabilité
- Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques
- Mesurer le niveau de sécurité d'un objet connecté
- Réaliser un test de pénétration

Public concerné

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.

Prérequis

Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux) et en programmation. Ou connaissances équivalentes à celles du cours Sécurité systèmes et réseaux, niveau 1 (réf. FRW).

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

PARTICIPANTS

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux) et en programmation. Ou connaissances équivalentes à celles du cours Sécurité systèmes et réseaux, niveau 1 (réf. FRW).

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

1 Rappel sur les IoTs (Object connectés)

- Les différents types d'IoT (Objets connectés).
- Les protocoles sans fil (WiFi...) et leurs portées (distance de fonctionnement). Liens avec M2M.
- Les architectures : ARM, MIPS, SuperH, PowerPC.

2 Le hacking et la sécurité

- Formes d'attaques, modes opératoires, acteurs, enjeux.
- Audits et tests d'intrusion.

3 L'environnement de l'IoT

- Réseau : 4G, LTE, LoRA, WiFi, MQTT, 802.11.15.4, ZigBee, Z-Wave, 6LoWPAN et BLE (Bluetooth LE).
- Application : Web App, Mobile App, Web, mobiles ou API (SOAP, REST).
- Firmware, le système d'exploitation de l'appareil : Windows, Linux x86/x64 bits ou Raspbian.
- Cryptage : protège les communications et les données stockées sur le périphérique.
- Matériel : puce, jeu de puces, Storagestorage, JTAG, ports UART, capteurs, caméra, etc.), port, capteur, caméra.
- Architecture : ARM, MIPS, SuperH, PowerPC.
- La structure du système, ses composants, sa protection et les mises à jour.

Travaux pratiques

Recueillir les informations (matériel, puce…) constituant l'objet connecté.

4 Les vulnérabilités

- La recherche de vulnérabilités.
- Les liaisons de l'objet connecté avec un réseau.
- Les mécanismes d'authentification.
- La recherche d'installation et mot de passe par défaut.
- La méthodologie des tests d'intrusion sur les IoTs (Objets connectés).
- Les outils : analyseurs logiques, débogueurs, désassembleurs et décompilateurs.

Travaux pratiques

Mesurer le niveau de sécurité d'un IoT (Objet connecté).

5 Les attaques

- Logiciel (XSS, SQLi, injection de commandes, exceptions mal traitées et attaques de corruption de mémoire RCE ou DoS).
- Matériels (JTAG, SWD, UART, SPI, bus I2C…).
- Connectivités sans fil, protocole de communication. Analyse d'émission.

Travaux pratiques

Accéder à un objet connecté via différentes attaques. Réaliser un test de pénétration.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

6 Le rapport d'audit

- Son contenu.
- Ses rubriques à ne pas négliger.

Travaux pratiques
Compléter un rapport pré rempli.

Dates et lieux

CLASSE À DISTANCE
2026 : 15 juin, 14 déc.