Hacking et Pentest : architectures embarquées

Cours Pratique de 4 jours
Réf : HAE - Prix 2022 : 2 790€ HT

L'architecture de base est la plupart du temps composée d'une unité centrale de traitement (CPU), d'un système d'exploitation (ou logiciel spécifique) et de sa connectivité : autant de composants vulnérables aux attaques qu'il faut évaluer et protéger sans oublier les contremesures à déployer.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant 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'une architecture embarquée

Réaliser un test de pénétration

LE PROGRAMME

dernière mise à jour : 06/2021

1) Rappel sur les architectures embarquées

- Système informatique ordinaire et système embarqué.
- Les différents types d'architectures embarquées.
- Les différentes contraintes liées à la solution embarquée.

2) Le hacking et la sécurité

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

3) L'environnement de l'embarqué

- Réseau : 4G, LTE, LoRA, WiFi, MQTT, 802.11.15.4, ZigBee, Z-Wave, 6LoWPAN et BLE (Bluetooth LE).
- 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.

4) Vulnérabilités des architectures embarquées

- La recherche de vulnérabilités.
- Les mécanismes d'authentification.
- Les liaisons d'un système embarqué avec son environnement (connectivité) : réseau, capteur et périphérique.
- Identifier et utiliser les applications et programmes hébergé sur un système embarqué.
- La méthodologie des tests d'intrusion.
- Les outils : analyseurs, débogueurs, désassembleurs et décompilateurs.

Travaux pratiques : Mesurer le niveau de sécurité d'une architecture embarquée.

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 stage "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.

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 stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage 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 stagiaire 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

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

5) Les attaques

- Les attaques physiques.
- Matériels : accès aux différents composants.
- Connectivités sans fil, protocole de communication. Analyse d'émission.
- Logiciel : structure du système de fichier, faille des applications hébergées, accès aux services via les applications.
- Mise à l'épreuve de la gestion des exceptions à l'aide d'un programme, attaques par épuisement.
- La reprogrammation du système.
- Introduction d'informations falsifiées.

Travaux pratiques : Accéder à un système embarqué via différentes attaques. Réaliser un test de pénétration.

6) Le rapport d'audit

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

Travaux pratiques : Compléter un rapport pré-rempli.

LES DATES

PARIS LA DÉFENSE
2022 : 05 avr., 27 sept., 29 nov.