HACKING ET PENTEST

500 € HT (tarif inter) | REF : RÉS19
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

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 san

5 JOURS
35 HEURES

OBJECTIFS

- 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..

PUBLIC | PRÉREQUIS

PUBLIC : Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.
PRÉREQUIS : Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux).

PROGRAMME

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..

Travaux pratiques : Quiz sur les architectures embarquées.

Le hacking et la sécurité

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

Travaux pratiques : Mise en situation professionnelle.

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 su.

Travaux pratiques : TP de fin de séquence.

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 .

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

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 appli.

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

Le rapport d'audit

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

Travaux pratiques : Compléter un rapport pré-rempli.

INFOS PRATIQUES

Méthodes pédagogiques
Alternance équilibrée de présentations, d'ateliers sur simulateur et de mises en situation dans des conditions similaires à celles de l'examen.

Modalités de l'évaluation initiale
Test de positionnement en amont de la session de formation.

Modalités d'évaluation finale
Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques.

Accessibilité aux personnes handicapés
Dans votre espace candidat, une rubrique dédiée au handicap vous permettra d'exprimer vos besoins d'adaptation afin que vous puissiez suivre votre formation dans les meilleures conditions.

Modalités et délais d'accès
L'inscription doit être finalisée 72 heures avant le début de la formation.

STATISTIQUES

Taux de satisfaction : 100%
Taux d'abandon : 0%

DATES ET LIEUX

Nous consulter