HACKING ET PENTEST - OBJETS CONNECTÉS IOT_1727

1300 € HT (tarif inter) | REF : -RÉS327
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

Sécurisation des objets connectés (IoT ou Internet Of Things)

2 JOURS | **14 HEURES**

PROGRAMME

RAPPEL SUR LES IOTS

- Les objets connectés..
- Les protocoles sans fil (WiFi...) et leurs portées (distance de fonctionnement). Liens avec M2M.
- Les architectures : ARM, MIPS, SuperH, PowerPC..

L'HACKING ET SÉCURITÉ

- Les différentes formes d'attaques..
- Audits et tests d'intrusion..

LES CADRES DE L'IOT

- Les réseaux et les applications..
- Le Firmware, le système d'exploitation de l'appareil : Windows, Linux x86/x64 bits ou Raspbian..
- Le cryptage, le matériel, l'architecture du système et ses composants..

LES VULNÉRABILITÉS

- L'exploration de vulnérabilités..
- La corrélation de l'objet connecté via le réseau..
- Les dispositifs d'authentification et la recherche d'installation et mot de passe..
- Les formalités des tests d'intrusion sur les objets connectés et les outils..

LES DIFFÉRENTES FORMES D'ATTAQUES

- Les logiciels, les matériels et les connectivités sans fils..

LE COMPTE RENDU

- Le contenu..
- Les catégories importantes..

OBJECTIFS

Rechercher des vulnérabilités sur l'ensemble de l'écosystème de l'objet connecté

PUBLIC | PRÉREQUIS

PUBLIC

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

PRÉREQUIS

Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux) et en programmation

INFOS PRATIQUES

HORAIRES DE LA FORMATION
de 9 h 00 à 12 h 30 et de 13 h 30 à 17 h 00
MÉTHODOLOGIE PÉDAGOGIQUE
Théorie | Cas pratiques | Synthèse
MODALITÉS D'ÉVALUATION
Évaluation qualitative des acquis tout au long de la formation et appréciation des résultats

DATES ET LIEUX

Aucune session ouverte