HACKING ET SÉCURITÉ

300 € HT (tarif inter) | REF : RÉS21
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

Cette formation vous apprendra les techniques avancées de hacking. Vous créerez des shellcodes et payload afin d'exploiter des vulnérabilités applicatives sur les systèmes d'exploitations afin de mieux comprendre les failles et pouvoir élever le niveau de

3 JOURS | **21** HEURES

OBJECTIFS

- Comprendre les récentes attaques et exploitations de système..
- Comprendre les techniques modernes de contournement des protections applicatives..
- Exploiter une vulnérabilité applicative sur les systèmes Linux et Windows..
- Créer des shellcodes et payloads (Linux et Windows)..

PUBLIC | PRÉREQUIS

PUBLIC : Responsables, architectes sécurité, administrateurs systèmes et réseaux. Pentesters.
PRÉREQUIS : Bonnes connaissances en sécurité SI, en C, Python et assembleur sont requises.

PROGRAMME

L'état de l'art offensif et défensif

- Un peu d'actualité : la 5G, la blockchain, le smart contract, IoTs (objets connectés), IA, IPv4, IPv6..
- Les dernières techniques d'attaques..
- Les dernières stratégies défensives..

Travaux pratiques : Exercice de défense.

Du C à l'assembleur au code machine

- Qu'est-ce que l'assembleur et le code machine. La compilation..
- Le fonctionnement d'un processeur..
- Les bases de l'assembleur et les bases du langage C..
- Les concepts de l'encodage (modes d'adressage, registres, instructions, opérations…)..

Travaux pratiques : TP en équipe.

Les attaques applicatives

- Les concepts des logiciels malveillants, des malwares (virus, rootkit ou autre)..
- État de l'art des backdoors sous Windows et Unix/Linux..
- Mise en place de backdoors et de trojans..
- Les shellcodes, le reverse shell TCP, le Bind Shell TCP..
- L'encodage de s.

Travaux pratiques : Exploitation de shellcode : buffer overflow (Windows ou Linux). Contourner des protections. Obtenir un shell root par différents types de buffer overflow. Utiliser Metasploit et générer des shellcode.

Les techniques d'analyse

- Analyse statique des binaires..
- Outils d'analyse dynamiques..
- La sécurité dans le bac à sable (sandboxing)..
- Le reverse engineering et debugging..
- Packers et crypters modernes..

Travaux pratiques : Analyse d'un malware avec les différentes techniques d'analyse.

La cryptanalyse

- Les concepts de la cryptanalyse (processus, chiffrement...)..
- Identification des algorithmes..
- Attaques sur le chiffrement par flux, sur les modes ECB et CBC..
- Les attaques par canaux cachés (side-channel attack)..
- Les attaques sur la blockchain..

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

HACKING ET SÉCURITÉ

300 € HT (tarif inter) | REF : RÉS21
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

Travaux pratiques : Quiz de fin de séquence.