Hacking et sécurité, niveau 2, expertise

Cours Pratique de 3 jours - 21h
Réf : HKE - Prix 2024 : 2 390€ HT

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 sécurité de votre système pour y remédier.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre les récentes attaques et exploitations de systèmes

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)

LE PROGRAMME

dernière mise à jour : 02/2019

1) 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.

2) 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…).

3) 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 shellcodes, suppression des NULL bytes.
- Exploitations de processus: buffer overflow, ROP, Dangling Pointers.
- Protections et contournement : flag GS, ASLR, PIE, RELRO, Safe SEH, DEP. Les shellcodes avec adresses hardcodées, LSD.
- Metasploit avancé : architecture, fonctionnalités, interfaces, workspaces, écriture d'exploit, génération de shellcodes.

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.

4) Les techniques d'analyse

- Analyse statique des binaires.
- Outils d'analyse dynamiques.

PARTICIPANTS

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

PRÉREQUIS

Bonnes connaissances en sécurité SI, en C, Python et assembleur sont requises.

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.

- 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.

5) 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.

LES DATES

CLASSE À DISTANCE	LILLE	PARIS
2024 : 24 juin, 08 oct., 11 déc.	2024 : 24 juin, 08 oct., 11 déc.	2024 : 17 juin, 01 oct., 04 déc.