Ethical Hacking, les failles applicatives
tutorat en option

Cours Pratique de 1 jour
Réf : 4ES - Prix 2021 : 35€ HT

Cette formation digitale a pour objectif de vous permettre d'identifier les techniques d'attaque utilisées dans les failles applicatives et d'être en mesure de préparer les contre-mesures adéquates. Elle s'adresse à un public de développeurs, RSSI ou DSI possédant des connaissances sur l'assembleur x86, le langage Python, l'architecture d'un ordinateur et la virtualisation. La pédagogie s'appuie sur un auto-apprentissage séquencé par actions de l'utilisateur sur l'environnement à maîtriser. Une option de tutorat vient renforcer l'apprentissage (disponible à partir de 2022).

OBJECTIFS PÉDAGOGIQUES

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

Connaître les principes de base des failles applicatives

Découvrir les outils permettant d'exploiter les failles applicatives sous Linux et sous Windows

Étudier l'exploitation de failles applicatives à distance

MÉTHODES PÉDAGOGIQUES

Formation digitale basée sur une pédagogie active avec une combinaison de théorie, de démonstrations, de partages d'expérience et de bonnes pratiques. Pour renforcer l'apprentissage, les séquences pédagogiques sont de courte durée et un tutorat est proposé en option.

TRAVAUX PRATIQUES

Exercice, quiz, fiche de synthèse, cours enregistrés et option de tutorat (débriefing, échanges par e-mail avec un expert, social learning, classe à distance sur mesure).

PARTICIPANTS

Développeurs, RSSI ou DSI.

PRÉREQUIS

Connaissances sur l'assembleur x86, le langage Python, l'architecture d'un ordinateur et la virtualisation.

COMPÉTENCES DU FORMATEUR

Les experts qui ont conçu la formation et qui accompagnent les apprenants dans le cadre d'un tutorat sont des spécialistes des sujets traités. 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. 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

L'évaluation est réalisée tout au long de la formation à travers différents moyens (QCM, exercices pratiques, quiz…). Le stagiaire évalue sa progression et ses acquis à l'issue de la formation.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : documentation et support de cours, exercices pratiques d'application et corrigés des exercices, études de cas ou présentation de cas réels. ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Une attestation de fin de formation est fournie si l'apprenant a bien suivi la totalité de la formation.

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 pshaccueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 08/2021

1) Comprendre le principe de base des failles applicatives

- Introduction.
- Contexte d'attaque.
- Segmentation de la mémoire.
- Assembleur.
- Gestion de la pile.
- Outils.
- Principe d'un buffer overflow.

2) Utiliser les outils

- Outils pour exploiter les failles applicatives sous Linux.
- Utilisation du débugger sous Linux.
- Utilisation du débugger sous Windows.
- Exploitation d'une faille sous Linux.

3) Maîtriser les failles applicatives à distance

- Exploitation d'une faille à distance.
- Écrasement du registre EIP.
- Création de la structure d'exploit.
- Incorporation d'un shellcode dans l'exploit.

4) Maîtriser les failles applicatives en local

- Exploitation d'une faille en local sur un logiciel.
- Détermination de l'écrasement de l'adresse retour.
- Protection SEH.
- Incorporation d'un shellcode dans l'exploit.