Ethical Hacking, connaître les techniques d'attaque utilisées dans les failles applicatives

Formation en ligne - 1h45
Réf : 4ES - Prix 2024 : 95€ HT

Ce cours en ligne 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. Il 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.

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

PÉDAGOGIE ET PRATIQUES

Une évaluation tout au long de la formation grâce à une pédagogie active mixant théorie, exercice, partage de pratique et gamification. Un service technique est dédié au support de l'apprenant. La formation est diffusée au format SCORM (1.2) et accessible en illimité pendant 1 an.

ACTIVITÉS DIGITALES

Démonstrations, cours enregistrés, partages de bonnes pratiques, quiz, fiches de synthèse.

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

La progression de l'apprenant est évaluée tout au long de sa formation au moyen de QCM, d'exercices pratiques, de tests ou d'échanges pédagogiques.
Sa satisfaction est aussi évaluée à l'issue de sa formation grâce à un questionnaire.

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 psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 06/2023

1) Connaître le principe de base des failles applicatives

- Définitions et types de failles.
- Présentation de Stack overflow et Heap overflow.

2) Découvrir le microprocesseur et les mémoires

- Fonctionnement des microprocesseurs.
- Registres.
- Mémoires.

3) Appréhender les bases du langage Assembleur

- Langage Assembleur.
- Pile (registres ESP, EBP et EIP).

4) Comprendre le buffer overflow

- Ability Server et Immunity Debugger.
- Fuzzing.
- Address Space Layout Randomization (ASLR).
- Shellcodes.

5) Exploiter la protection SEH

- Ecrasement SEH.
- Protection SEH.