Hacking éthique, pentesteur niveau 1 (BV-CEHP1), certification Bureau Veritas

Cours Pratique de 5 jours - 35h
Réf : THH - Prix 2024 : 3 850€ HT

OBJECTIFS PÉDAGOGIQUES

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

Comprendre la méthodologie du hacker

Apprendre le vocabulaire lié au Hacking

Mettre en pratique le cycle de l'attaquant

Rédiger un rapport de pentest

CERTIFICATION

Partie théorique et pratique. Le temps destiné au passage de la certification est de 3H. L'examen est composé de 3 parties : QCM, mise en situation sur points spécifiques, mise en situation sur cas concrets. Il peut se dérouler à distance.

PARTENARIAT

La certification est délivrée par Bureau Veritas Certification.
ORSYS et Bureau Veritas Certification se sont associés pour construire une offre de certifications couvrant les principaux domaines de la cybersécurité : architectures sécurisées, sécurité offensive et défensive, sécurité organisationnelle et système de management.

LE PROGRAMME

dernière mise à jour : 02/2022

1) Principe et méthodologie du Hacking

- Définition.
- Typologie des attaquants.
- Vocabulaire.
- PTES.
- OWASP.
- OSSTMM.
- Red Team / Blue Team.
- Kill Chain unified.

2) Préparation audit + rapport

- Contrat.
- Contexte et périmètre.
- Rappels des lois en vigueur.
- La trousse à outil d'un pentesteur.
- Mise en place dans le cloud.
- Comment s'organise un rapport.

3) Vecteurs d'attaques

- Virus / ver / cheval de troie.
- Backdoor.
- Logiciel espion / Keylogger.
- Exploit.
- Rootkit.

PARTICIPANTS

Techniciens et administrateurs systèmes et réseaux, architectes sécurité, intégrateurs sécurité, personnes étudiant la cyber-sécurité, responsables sécurité, auditeurs sécurité

PRÉREQUIS

Avoir suivi le cours "Intégrateur sécurité réseaux niveau 1 (BV-CISR1), certification Bureau Veritas" réf. SRE ou posséder les connaissances équivalentes

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.

- Ransomware.
- Pourriel / Hameçonnage / Canular informatique.
- Spearphishing.
- Botnet.
- Scanner de réseaux et de failles.

4) OSINT
- Présentation OSINT.
- Méthodologie OSINT.
- Exemples : Google dorks, recherche d'emails, recherche de sous-domaines.

5) Reconnaissance active et vulnérabilités
- Principe.
- Méthodologie.
- Pratique : Nmap, metasploit, scapy.
- MITRE ATT&CK.
- Scanner de vulnérabilités.
- Social ingénierie.
- CVE.
- Défaut de configuration.

6) Typologie des attaques
- Exploitation réseau (MITM).
- Social ingénierie / Phishing / Deepfake.
- Server side (Exploit CVE, Cracking + Bruteforce).

7) Hacking Web & Application Web, attaques avancées
- Principe.
- Méthodologie.
- Typologie d'attaque : Client side, Back side.
- TOP10 OWASP.
- Exploitation de failles.
- Création de Payload.
- Customiser ses exploits.
- Mise en œuvre du Pivoting.
- Exploitation Browser.

8) Post-exploitation, rapport
- Mise en œuvre de techniques d'exfiltration.
- C&C.
- Les élévations de privilège.
- Effectuer une énumération locale.
- Effacer ses traces.
- Exemple et étude d'un rapport.
- Communication et résultats.

9) Mise en situation, focus sur des technologies spécifiques
- Pentest d'un lab.
- Rédaction du rapport.
- Hack Wifi.
- Hack Cloud.
- Hack IoT.
- Hack Mobile.

10) Examen
- Révisions, examen blanc.

- Examen final.

LES DATES

CLASSE À DISTANCE
2024 : 13 mai, 15 juil., 04 nov.

PARIS
2024 : 22 avr., 08 juil., 21 oct.