Certified Lead Ethical Hacker, certification PECB

Cours Pratique de 4 jours - 28h
Réf : CEY - Prix 2024 : 3 940€ HT

Vous acquérez les connaissances et les compétences nécessaires pour planifier et réaliser des pentest internes et externes, en conformité avec différents référentiels (PTES, OSSTMM) ainsi que la rédaction de rapport et proposition de contre-mesure. Le cours est compatible avec la rubrique Protect and Defend du NICE.

OBJECTIFS PÉDAGOGIQUES

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

Comprendre le mécanisme des principales attaques

Détecter les fragilités d'un système par la connaissance des différentes cibles d'un piratage

Appliquer des mesures et des règles basiques pour lutter contre le hacking

Rédiger un rapport de pentest

CERTIFICATION

Après avoir acquis l'expertise nécessaire avec ce cours, vous passerez l'examen "PECB Certified Lead Ethical Hacker". L'examen, d'une durée de 6 heures en distanciel, comprend deux parties : l'examen pratique et la rédaction du rapport. L'examen pratique exige du candidat qu'il compromette au moins deux machines cibles au moyen des tests d'intrusion. Le processus doit être documenté dans un rapport écrit. L'examen PECB Certified Lead Ethical Hacker est un examen à livre ouvert. Les candidats sont autorisés à utiliser les supports de cours et leurs notes personnelles pendant l'examen. Le certificat PECB atteste que vous avez acquis les capacités nécessaires pour les tests de pénétration selon les meilleurs référentiels.

PARTICIPANTS

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

PRÉREQUIS

Bonnes connaissances en réseaux et systèmes (Microsoft et Linux).

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.

LE PROGRAMME

dernière mise à jour : 02/2022

1) Cybersécurité et architecture

- Panorama de la cybersécurité et architecture contemporaine.
- Effectuer un test d'intrusion, un pentest, les différents types de pentest.
- Les architectures, les systèmes d'exploitations, les failles connues.

2) La reconnaissance active

- Les formes de reconnaissance, active et passive.
- La reconnaissance, le scanning et l'énumération.
- Collecter des informations sur ses vulnérabilités.
- Balayage des ports.
- Exploiter des failles de sécurité connues des services rattachés aux ports, etc.

Travaux pratiques : Revue des vulnérabilités automatiques : Nessus, OpenVAS.

3) L'exploitation des systèmes

- Les frameworks d'exploitation.
- Compréhension des CVEs : les types (Remote, Local, Web).
- Exploitations de processus: Buffer Overflow, ROP, Dangling Pointers.
- Les shellcodes, les rootkits.

- Attaque des authentifications Microsoft, PassTheHash.
- Windows : Buffer Overflow à la main, les exploits.

Travaux pratiques : Exploiter les failles des systèmes (Microsoft et Linux).

4) L'exploitation et la post-exploitation

- Préparation du document et écriture du rapport.
- Décrire les vulnérabilités trouvées.
- Formuler les recommandations de sécurité.

Travaux pratiques : Rédaction et mise en forme du rapport.

LES DATES

CLASSE À DISTANCE
2024 : 10 sept., 10 déc.

PARIS
2024 : 21 mai, 03 sept., 17 déc.

BRUXELLES
2024 : 10 sept., 10 déc.

LUXEMBOURG
2024 : 10 sept., 10 déc.