Certified Lead Ethical Hacker (formation et examen de certification)

Module 921 – Lead Ethical Hacker

Objectifs

La formation Certified Lead Ethical Hacker vous permettra d'acquérir l'expertise nécessaire pour maîtriser le hacking éthique.
Durant cette formation, vous acquerrez des connaissances approfondies sur les outils utilisés par les hackers, sur comment organiser une veille technique capable d'analyser les vulnérabilités sur les principaux OS vous serez apte à bien exploiter Active Directory et savoir comment contourner les antivirus.
La formation se conclut par un examen donnant lieu à une certification Lead Ethical Hacker

A qui s'adresse ce cours

Ce stage s'adresse aux spécialistes des TI et aux personnes en charge de la cybersécurité et qui cherchent à maîtriser les techniques de piratage éthique et de test d'intrusion,

Cours de 5 jours – 2 950 € HT

Paris
21 juin 2021
29 nov.
28 fév. 2022
25 avril

Lyon
21 juin 2021
28 fév. 2022

Intra entreprise
Sur demande
*Examen de certification inclus
Formation à distance possible (hors examen)

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

Certification enregistrée RS3716
https://www.francecompetences.fr

Pour vous inscrire

Téléphone : 01 40 33 76 88
E-mail : contact@beresilientgroup.com

Courrier

BRG – 10, rue Emile Landrin – 75020 Paris
Centre de formation agréé préfecture : 11754161975
SAS au Capital de 150 000 Euros - Siret Paris B 441 951 845

Contenu du module 921

Jour 1 Introduction, outils et environnement

- Objectifs et structure de la formation
- Principes fondamentaux du hacking éthique
- Metasploit
- Cobalt Strike

Jour 2 Exploitation système et mémoire, reverse shell

- Exploitation des principaux OS
- Reverse connexion et reverse shell
- Fonctionnement d'un programme en mémoire
- Bufferoverflow
- Moyens de sécurité et contournement

Jour 3 Pivoting, post exploitation, spécificités Microsoft

- Pivoting (avec SSH, multiniveaux)
- Meterpreter PortFoward
- Principes fondamentaux de la post exploitation
- Post exploitation selon les principaux OS
- Utilisation d'Empire
- Fonctionnement d'un domaine Microsoft
- Exploitation des credentials et de Kerberos

Jour 4 Introduction, outils et environnement

- Ecriture de code Recompilation de Meterpreter
- Application Whitelist bypass Powershell Obfuscation
- Principe d'exfiltration de données
- Utilisation de Cloakify Factory
- Exfiltration de données (par DNS, avec Empire)
- OWASP Top 10 des failles de sécurité.
- Clôture de la formation

Jour 5 Examen de certification

brg be resilient group

Mise à jour du 30/04/2021

Module 921

Certified Lead Ethical Hacker (formation et examen de certification)

Module 921 – Lead Ethical Hacker

Prérequis

Le candidat doit avoir des connaissances fondamentales de la sécurité de l'information, il doit posséder de solides compétences sur les systèmes d'exploitations (Microsoft, Linux).
La certification est accessible aux personnes disposant d'au moins cinq années d'expérience

Modalités et délais d'accès

1. Contacter nous par mail ou téléphone pour qualifier votre besoin de formation
2. Renvoyez le bon de réservation complété (disponible à la fin du catalogue)
2. Validation de votre inscription (éligibilité du stagiaire)
3. Etablissement et signature de la convention de formation
4. Envoi de votre convocation à la session de formation avec les détails (horaires, lieu…)

Durée estimée entre la demande du bénéficiaire et le début de la prestation: de 1 à 3 mois

Méthodes mobilisées

Cours magistral basé sur les meilleures pratiques liées à la mis en œuvre de tests d'intrusion
Exercices pratiques panachés de travaux dirigés et guidés par l'apprenant et d'exercices en pleine autonomie, afin d'assurer une assimilation des savoir-faire requis.
Support de cours au format papier et numérique, version française

Modalités d'évaluation – Validation des compétences - Certification

Examen de certification 3 heures - Organisme certificateur PECB
Evaluation de la totalité des cinq compétences constitutives de la certification :
- Simuler l'attaque d'un système d'information d'entreprise par un utilisateur malintentionné ou un logiciel malveillant, afin de détecter les fragilités de celui-ci.
- Concevoir et mettre en œuvre une série de tests d'intrusion à même de situer le degré de risque représenté par chacune des fragilités identifiées.
- Rédiger un rapport de pentest présentant l'ensemble des vulnérabilités exploitables dans les configurations ou la programmation, en vue de la conception par les responsables d'un plan d'amélioration de la sécurité du système d'information cohérent avec l'échelle des risques.
- Identifier et chiffrer les parades adaptées aux menaces, afin de faciliter la prise de décision et la mise au point du plan de sécurité.
- Conseiller une entreprise sur les bonnes pratiques en matière de détection et de lutte contre le piratage, afin de faciliter la mise en place des mesures et procédures adéquates.

Equivalences, passerelles, suite de parcours et débouchés

Pas de certification partielle – Remise d'un certificat de compétences PECB valable 3 ans
La certification permet aux individus de disposer des compétences nécessaires à la conception et à la mise en œuvre de tests d'intrusion sur différents types de systèmes d'information. Répondre aux exigences de postes correspondants à ces caractéristiques : RSSI, chefs de projet/consultant en sécurité des systèmes d'information. La certification permet aux entités utilisatrices de faciliter la gestion des compétences et le recrutement en s'appuyant sur une certification reconnue. Favoriser la collaboration inter-organisationnelle en partageant un langage et des processus communs. Garantir aux parties prenantes de l'organisation un certain standard de qualité. Le maintien dans le temps de la certification garantit la transférabilité des compétences d'une entité utilisatrice à une autre.
Suite de parcours: ISO 27001 Lead Implementer/Auditor, Cyber-résilience

Accessibilité aux personnes handicapées

Procédure Accueil Handicap: En cas d'accueil d'un stagiaire handicapé, l'office manager de BRG est le référent handicap, qui pourra si besoin mobiliser notre réseau de partenaires du champ du handicap.
Accessibilité aux personnes à mobilité réduite: Nos locaux sont Etablissement Recevant du Public (ERP)
Attestation de vérification de l'accessibilité aux personnes handicapées – Dossier accessibilité

brg
be resilient group

Mise à jour du 30/04/2021