Certified Advanced Lead Ethical Hacker

Référence : **SECCALEH** Durée : **5 jours** Certification : **PECB**

Code CPF : **RS3716**

CONNAISSANCES PREALABLES

• 1-Connaissance pratique des systèmes Linux, Windows. • 2-Connaissance pratique des réseaux et du modèle OSI. • 3-Connaissance du cycle de l'attaquant et des principaux outils utilisés. • 4-Tous les candidats devront présenter une carte d'identité valide avec une photo lors du passage de l'examen.

PROFIL DES STAGIAIRES

• Professionnels de la cybersécurité. • Spécialistes des TI.

OBJECTIFS

• Connaitre les outils utilisés par les Hacker. • Savoir organiser une veille technique. • Être capable d'analyser les vulnérabilités sur les systèmes Linux et Windows. • Maîtriser l'exploitation et la post-exploitation des différents environnements. • Mesurer l'importance de bien exploiter Active Directory. • Comprendre comment contourner les antivirus. • Préparer et passer l'examen de certification "CALEH, Certified Advanced Lead Ethical Hacker" du PECB.

CERTIFICATION PREPAREE

- Certified Advanced Lead Ethical Hacker. Pour en savoir plus sur cette certification, cliquez ici et accédez aux informations complètes fournies par France Compétences

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Outils et environnement des attaquants

- L'utilisation de Metasploit : installation, premier lancement, Armitage Team Server, configuration
- Utilisation de Cobalt Strike : planification, introduction à l'outil, Cobalt Strike interface et team server

Reverses Shell et exploitation système

- Les exploitations Windows
- Les exploitation Linux
- Introduction aux reverse connexion
- Introduction aux reverse shell

Bufferoverflow

- Compréhension de la mémoire
- Étude du fonctionnement d'un programme en mémoire
- Exploitation simple bufferoverflow
- Étude des moyens de sécurité et contournement

Pivoting

- Pivoting avec SSH
- Meterpreter PortFoward
- Pivoting multi-niveau

Introduction à empire et post-exploitation

- Installation et configuration
- Fondamentaux
- Post-Exploitation Windows
- Post-Exploitation Linux

Spécificités des domaines Microsoft

- Fonctionnement d'un domaine
- Exploitation des credentials
- Exploitation des vulnérabilité/fonctionnalité de Kerberos

Contournement d'antivirus et systèmes de détection

- Ecriture de code
- ShellCode vs DLLs Client/Serveur
- Recompilation de Meterpreter
- Application Whitelist bypass
- Powershell Obfuscation

Exfiltration des données

- Principe d'exfiltration de données
- Cloakify Factory
- Exfiltration de données par DNS
- Exfiltration avec Empire

Etude et exploitation du top 10 OWASP

Examen PECB Certified Advanced Lead Ethical Hacker

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans les investigations légales informatiques.
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales.
- Les tests pratiques sont similaires à l'examen de certification.
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré.
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- L'examen couvre les domaines de compétences suivants : Domaine 1 : Connaissance des outils - Domaine 2 : Recherche de vulnérabilités sur un système Linux et Windows - Domaine 3 : Compréhension et exploitation d'une vulnérabilité sur un système Linux et Windows - Domaine 4 : Compréhension et exploitation de vulnérabilités liées aux domaines - Domaine 5 : Exfiltration des données - Domaine 6 : Conto