Certified Lead Ethical Hacker

★★★★★

SII-422 **5 Jours (35 Heures)**

Description

Cette formation prépare à la certification PECB Lead Ethical Hacker.

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.

À qui s'adresse cette formation ?

Pour qui

Responsables, architectes sécurité.

Techniciens et administrateurs systèmes et réseaux.

Prérequis

Basic knowledge of a Linux and Windows system

Knowledge of networks and OSI model

Les objectifs de la formation

- Comprendre et connaître les référentiels liés au pentest
- Prendre connaissance des outils et source de veille
- Savoir mener une analyse de vulnérabilité sur un système Linux et Windows
- Comprendre l'exploitation et la post-exploitation des différents environnements
- Préparer et passer l'examen de certification "CLEH, Certified Lead Ethical Hacker" du PECB

Programme de la formation

Introduction

- Panorama et faits marquants (WannaCry, NotPetya, Facebook)
- Les composants de la sécurité (CID)
- Les types et référentiels du Pentest : BlackBox / GreyBox / White / RedBlue Team - PTES , OSSTM (OWASP)
- Le cycle de l'attaquant
- La trousse à outil et l'environnement : Kali (Site de Kali et système), étude de l'environnement, conservation des résultats (Utilisation de keepnote ou équivalent)

Intelligence Gathering

- Les principes de la recherche Internet/Passive (OSINT) : exemple de cas
- Recherche sur l'organisation : physique, logique, organisation, électronique, recherche infrastructure, finance
- Recherche sur l'employé : social network, présence sur internet
- Reconnaissance externe : reconnaissance passive (Recherche DNS et BGP), reconnaissance Active (Scan des services, Scan des versions, Scan des OS, Recherche des services avancée, AXFR, SMTP, DNS_BF etc...)
- Reconnaissance interne : énumération du réseau courant (ARP/ICMP), le focus interne

Modélisation et analyse des vulnérabilités

- Etude et compréhension des CVEs : les types (Remote , Local , Web)
- Examen et revue des vulnérabilités manuels : NMAP ? CVE DETAILS
- Examen et revue des vulnérabilités automatiques : Nessus, Openvas, NSE
- Bilan et cartographie

Exploitation

- Les exploitations réseaux courantes : le man in the middle, fake DHCP
- Client exploitation : les attaques courantes sur l'humain (le navigateur, attaque sur les fichiers, USB)
- Exploitation des services et OS : mauvaise configuration - tous systèmes (Default password, Anonymous ftp), Windows (Buffer Overflow à la main, exploitation connue à l'aide d'exploit-db), Linux (exploitation connue à l'aide d'exploit-db)

Post - Exploitation

- Élévation des privilèges : Windows (Linux)
- Persistence / Backdoor : mise en place de backdoor sous Windows et Linux, Cron, Scheduled Task
- Pivoting et rebond
- Exfiltration de données

Préparation et passage de l'examen de certification PECB Certified Lead Ethical Hacker

- Révision des concepts en vue de la certification
- Examen blanc
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétence suivants : Domaine 1 : Principes et concepts fondamentaux du piratage éthique - Domaine 2 : Mécanismes d'attaque - Domaine 3 : Principes et référentiels sur les tests d'intrusion - Domaine 4 : Planifier et effectuer des tests de pénétration en utilisant divers outils et techniques - Domaine 5 : Rédaction de rapports de tests d'intrusion
- L'examen comprend deux parties. La première partie est un examen sur papier, qui consiste en des questions de type dissertation. La deuxième partie est plutôt technique, dans laquelle le candidat devra effectuer des exercices de test d'intrusion sur ordinateur et rédiger un rapport d'analyse
- Les participants sont autorisés à utiliser leurs notes personnelles lors de l'examen sur papier et lors de la partie pratique de l'examen