

- *Connaitre les outils utilisés par les Hacker*
- *Savoir organiser une veille technique*
- *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*

**5**

Prix : € / HT

**OUTILS PÉDAGOGIQUES****PUBLIC VISÉ**

- Professionnels de la cybersécurité
- Spécialistes des TI

**MODALITÉS D'ÉVALUATION****MODALITÉS DE FINANCEMENT****MODALITÉS ET DÉLAIS D'ACCÈS****OBJECTIFS PÉDAGOGIQUES****ACCESSIBILITÉ****LES POINTS FORTS DE LA FORMATION****PRÉ-REQUIS**

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

**MODALITÉS ET DÉLAIS D'ACCÈS****ATTESTATION OBTENUE****EFFECTIF DE LA FORMATION****CERTIFICATION****MODALITÉ PÉDAGOGIQUE**

Cours dispensé en mode présentiel avec une alternance d'apports théoriques et méthodologiques, et de mises en situations pratiques

**PROCHAINES SESSIONS**

Nous consulter.  
Nous consulter.  
Nous consulter.

**PROGRAMMES DE CALEH, CERTIFIED ADVANCED LEAD ETHICAL HACKER****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 PortForward
- 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 SYSTÈME DE DETECTION

- 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 WINDOWS FORENSICS MANAGER

- 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
- Les candidats sont autorisés à utiliser les supports de cours mais aussi les notes qu'ils auront prises
- 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 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 : Contournement de l'antivirus et développement d'outil

