Formation Lead Pen Test Professional

Module 1 : Introduction aux tests d'intrusion et planification

- Principes fondamentaux des tests d'intrusion
- Éthique, légalité et conformité dans le pen testing
- Définition du périmètre et des objectifs du test
- Collecte d'informations préliminaires et reconnaissance
- Élaboration du plan de test d'intrusion

Module 2 : Connaissances techniques fondamentales

- Fonctionnement des réseaux et protocoles
- Systèmes d'exploitation (Linux, Windows)
- Concepts de sécurité et points d'entrée typiques
- Outils essentiels pour les tests (Nmap, Wireshark, Metasploit…)
- Environnement de test : préparation et configuration

Module 3 : Réalisation pratique du test d'intrusion

- Scanning et analyse des vulnérabilités
- Exploitation des failles (privilege escalation, accès non autorisé, injections…)
- Tests sur les applications Web, infrastructures réseaux, et systèmes
- Attaques sur les services, applications mobiles et IoT
- Techniques d'ingénierie sociale (phishing, pretexting…)

Module 4 : Analyse, rapport et recommandations

- Organisation et interprétation des résultats
- Rédaction de rapports professionnels de tests d'intrusion
- Proposition de recommandations concrètes
- Présentation des résultats à différents types d'interlocuteurs
- Gestion des actions correctives et suivi post-audit

Module 5 : Examen de certification

- Révision des modules et questions de mise en situation
- Préparation à l'examen PECB Lead Pen Test Professional
- Passage de l'examen