Sécurité Technique

Préparation Offensive Security Certified Professional (OSCP)

La préparation à la certification Offensive Security Certified Professional (OSCP) vous permettra d'acquérir des compétences pratiques et solides en tests d'intrusion sur des réseaux et systèmes réels. Vous apprendrez à identifier, exploiter et documenter des vulnérabilités dans divers environnements, en utilisant une approche méthodique et rigoureuse. Cette formation met l'accent sur la compréhension des fondamentaux du hacking éthique, le développement de techniques d'exploitation variées, et la rédaction de rapports clairs et professionnels. En maîtrisant ces compétences, vous serez capable de mener des audits de sécurité efficaces et de démontrer votre expertise en sécurité offensive de manière reconnue internationalement.

Public visé

- Professionnels de la cybersécurité souhaitant acquérir des compétences pratiques en tests d'intrusion.
- Administrateurs systèmes et réseaux désireux de comprendre les techniques d'attaque.
- Développeurs souhaitant renforcer la sécurité de leurs applications.
- Toute personne aspirant à une carrière en sécurité offensive.

Les objectifs de la formation

- Maîtriser les méthodologies et techniques de tests d'intrusion en environnement réel.
- Utiliser efficacement les outils de Kali Linux pour identifier et exploiter des vulnérabilités.
- Développer des compétences en élévation de privilèges sur systèmes Windows et Linux.
- Rédiger des rapports professionnels de tests d'intrusion.
- Préparer et réussir l'examen de certification OSCP.

Les prérequis de la formation

- Connaissances de base en réseaux et systèmes d'exploitation (Windows et Linux).
- Familiarité avec la ligne de commande et les scripts.
- Compréhension des concepts fondamentaux de la cybersécurité.
- Aucune certification préalable requise, mais une expérience en IT est recommandée.

Programme de la formation

Module 1 :
- Introduction à la cybersécurité

Module 2 :
- Stratégies d'apprentissage efficaces

Module 3 :
- Rédaction de rapports pour les testeurs d'intrusion

Module 4 :
- Collecte d'informations

Module 5 :
- Analyse de vulnérabilités

Module 6 :
- Attaques sur applications web

Module 7 :
- Injection SQL

Module 8 :
- Attaques côté client

Module 10 :
- Utilisation d'exploits publics

Module 11 :
- Évasion des antivirus

Module 12 :
- Attaques par mot de passe

Module 13 :
- Élévation de privilèges Windows

Module 14 :
- Élévation de privilèges Linux

Module 15 :
- Redirection de ports et tunneling SSH

Module 16 :
- Framework Metasploit

Module 17 :
- Active Directory

Module 17 :
- Laboratoires de challenge