Sécurité Technique

Pentesting – Réaliser des tests d'intrusion

A l'issue de la formation, le stagiaire sera capable mettre en place une procédure pour réaliser des tests d'intrusion.

Public visé

- RSSI,
- Techniciens,
- Auditeurs amenés à faire du pentest, Administrateurs systèmes et réseaux.

Les objectifs de la formation

- Comprendre les fondamentaux et le cadre juridique du pentesting.
- Connaître les différentes phases d'un test d'intrusion.
- Utiliser les outils et techniques d'analyse de pentesting.
- Simuler des attaques.
- Rédiger un rapport d'audit professionnel.

Les prérequis de la formation

- Des notions en informatique et sécurité des systèmes d'information.

Méthodes pédagogiques

- Apports théoriques structurés, illustrés par des exemples concrets et adaptés au contexte professionnel des participants.
- Exercices pratiques et ateliers à chaque étape pour favoriser l'appropriation des connaissances.
- Étude de cas permettant de relier les différents blocs de compétences.
- Forte interaction entre les formateurs et les stagiaires permettant de rendre les échanges plus concrets, en corrélation avec les attentes des stagiaires.
- Documentation pédagogique complète, fournie au format numérique.
- Questionnaire d'évaluation du cours en fin de formation, analysé par notre équipe pédagogique.
- Attestation des compétences acquises transmise au stagiaire à l'issue de la formation.
- Attestation de fin de formation adressée en même temps que la facture à l'entreprise ou à l'organisme financeur, confirmant la participation complète du stagiaire à la session.

Programme de la formation

Jour 1 :

- **Matin :** Objectifs de la formation / Définitions (pentest vs audit) / Cadre légal & principes de la sécurité / Quiz de validation
- **Après-midi :** Méthodologies et approches de pentest / Planification & périmètre / Cycle de vie d'un test / Étude de cas / Quiz

Jour 2 :

- **Matin :** Reconnaissance passive (OSINT) / Cartographie des actifs / Outils comme Whois, Shodan, Maltego / Quiz
- **Après-midi :** Reconnaissance active / Scans réseau & vulnérabilités (Nmap, Nessus, OpenVAS…) / Exercices pratiques de détection de failles / Quiz

Jour 3 :

- **Matin :** Tests d'exploitation des vulnérabilités / Exploitation manuelle vs automatisée / Introduction à Metasploit et autres frameworks / Quiz
- **Après-midi** : Tests sur infrastructures systèmes & réseau / Applications web (SQLi, XSS, CSRF, LFI/RFI) / Applications mobiles / Labs pratiques / Quiz

Jour 4 :

- **Matin :** Techniques avancées : élévation de privilèges, pivoting, persistance / Ingénierie sociale / Sécurité physique / Quiz
- **Après-midi :** Post-intrusion : exploitation, validation, collecte de preuves / Exercices de type Capture The Flag (CTF) / Quiz

Jour 5 :

- **Matin :** Analyse et documentation des résultats / Rédaction de rapport d'audit professionnel / Restitution aux décideurs et techniciens / Quiz
- **Après-midi :** Plans d'action correctifs et suivi / Mise en situation et évaluation des compétences / Bonnes pratiques pour pérenniser un processus de pentesting / Clôture et évaluation finale / Remise des attestations

5 Jours
35 Heures

Sur demande

+33 1 89 62 34 30

formation@acgcybersecurity.fr

Campus Cyber, Tour Eria, 5 Rue Bellini 92800 Puteaux, FRANCE

Toutes nos formations sont accessibles aux personnes en situation de handicap.

ACG CyberAcademy