PROGRAMME DE FORMATION

Tests d'intrusion et hacking éthique : les fondamentaux

Cybersécurité & Protection des données

RÉFÉRENCE	VERSION	ÉDITION	DOMAINE
WF-0462	V2026-004	3 novembre 2026	Cybersécurité & Protection des données

DURÉE	MODALITÉ	PROGRAMME	SANCTION
35 h	Distanciel asynchrone (e-learning)	8 modules 18 leçons	Attestation et certificat de réalisation

Objectifs pédagogiques

À l'issue de la formation, l'apprenant sera capable de :

- expliquer le cadre légal du test d'intrusion : aucun test sans autorisation écrite et préalable du propriétaire du système, dans un périmètre et une période définis ;
- situer les infractions pénales d'atteinte aux systèmes de traitement automatisé de données et les règles déontologiques du métier ;
- décrire les phases d'une mission de test d'intrusion et les référentiels méthodologiques courants, dont ceux de l'OWASP ;
- mettre en place un laboratoire isolé pour s'exercer sur des cibles prévues à cet effet ;
- reconnaître les grandes familles de vulnérabilités des applications web, des systèmes et des réseaux ;
- évaluer la gravité d'une vulnérabilité et proposer des mesures de correction ;
- rédiger un rapport de test d'intrusion clair, à destination des équipes techniques et de la direction.

L'essentiel de la formation

Public visé

Administrateurs systèmes et réseaux, développeurs et techniciens réseau souhaitant comprendre la démarche du test d'intrusion pour mieux sécuriser les systèmes dont ils ont la charge.

Prérequis

- Intermédiaire : bonne pratique de l'informatique, des réseaux ou du développement ; débutant en test d'intrusion.
- Connaître les bases des réseaux (adressage IP, protocoles courants)
- Savoir utiliser la ligne de commande d'un système Linux ou Windows
- Avoir des notions de fonctionnement des applications web
- Disposer d'un ordinateur capable de faire fonctionner des machines virtuelles, d'une connexion Internet et d'une adresse électronique

Modalités et déroulement

Formation à distance sur la plateforme WILL FORMATION, avec accès individuel aux contenus, exercices et quiz, en entrées et sorties permanentes. Des classes virtuelles animées par un formateur complètent les contenus en ligne. Les exercices pratiques se déroulent exclusivement dans un laboratoire isolé, sur des cibles prévues à cet effet. Un accompagnement pédagogique est assuré pendant toute la durée du parcours.

Méthodes pédagogiques

- Apports théoriques, juridiques et méthodologiques
- Démonstrations commentées en environnement de laboratoire
- Exercices pratiques sur des cibles d'entraînement volontairement vulnérables
- Études de cas et rédaction de rapports
- Classes virtuelles de correction et d'échange
- Quiz de validation des acquis
- Accompagnement pédagogique à distance

Répartition du temps de formation : **19 %** théorique · **57 %** pratique · **24 %** évaluation

Moyens pédagogiques et techniques

- Plateforme de formation en ligne accessible en continu
- Supports de cours consultables et téléchargeables
- Guide d'installation d'un laboratoire virtuel isolé
- Modèles de lettre d'autorisation et de rapport
- Outil de classe virtuelle
- Messagerie pour joindre l'équipe pédagogique

Modalités d'évaluation

- Positionnement initial en début de parcours
- Évaluations formatives tout au long du parcours (quiz, exercices en laboratoire)
- Évaluation finale des acquis : étude de cas et rédaction d'un rapport en fin de parcours

Sanction

Une attestation de fin de formation et un certificat de réalisation sont remis au participant sous réserve de la réalisation du parcours.

Cette formation n'est pas présentée comme préparant à une certification enregistrée : elle ne comprend ni inscription ni présentation à des épreuves de certification, et n'ouvre droit à aucune délivrance de certification ni au financement par le CPF.

Modalités et délais d'accès

La demande d'inscription peut être effectuée par téléphone, par courrier électronique ou au moyen du formulaire en ligne.

Un entretien ou un questionnaire de positionnement permet de vérifier l'adéquation de la formation avec les besoins, le niveau initial et les prérequis du candidat.

L'inscription devient définitive après validation du dossier administratif, acceptation des documents contractuels et, le cas échéant, confirmation du financement.

Les accès à la plateforme sont généralement activés sous 48 à 72 heures ouvrées après validation complète du dossier.

Les formations à distance sont proposées en entrées et sorties permanentes, sous réserve des délais ou dates imposés par le financeur ou le certificateur.

Accessibilité aux personnes en situation de handicap

Les personnes en situation de handicap sont invitées à signaler leurs besoins lors de leur demande d'inscription. Une étude personnalisée est réalisée afin de définir les adaptations pédagogiques, techniques ou organisationnelles appropriées. Lorsque le besoin ne peut pas être satisfait directement, une orientation vers un partenaire ou une structure spécialisée est proposée.

Référent handicap : **handicap@will-formation.com**

Tarif de la formation

Prix : **2 770 €**

Financement : prise en charge possible par les organismes financeurs, selon les critères d'éligibilité applicables.

Qualiopi processus certifié

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION. Certificat QUA25070009. WILL FORMATION — Société par actions simplifiée à associé unique au capital de 30 000 € — NDA 11757059675 (cet enregistrement ne vaut pas agrément de l'État) — SIRET 893 713 180 00014 — 01 85 09 25 99 — info@will-formation.com — www.will-formation.com

Programme détaillé

8 modules, 18 leçons — durée totale 35 h.

01 Cadre légal, éthique et contractuel du test d'intrusion

1. Atteintes aux systèmes de traitement automatisé de données : ce que dit la loi
2. Autorisation écrite du propriétaire, périmètre et convention de test
3. Déontologie, confidentialité et gestion des données découvertes

02 Méthodologie d'une mission de test d'intrusion

1. Types de tests et phases d'une mission
2. Référentiels méthodologiques et ressources de l'OWASP

03 Laboratoire d'entraînement isolé

1. Machines virtuelles, réseau isolé et distribution Linux spécialisée
2. Cibles d'entraînement volontairement vulnérables et règles d'usage

04 Reconnaissance et cartographie dans le périmètre autorisé

1. Collecte d'informations et respect du périmètre
2. Cartographie des services exposés en laboratoire

05 Vulnérabilités des applications web

1. Grandes familles de vulnérabilités web et leurs causes
2. Mise en évidence en laboratoire et bonnes pratiques de développement sécurisé

06 Vulnérabilités des systèmes et des réseaux

1. Défauts de configuration et services vulnérables
2. Gestion des mots de passe, des droits et des mises à jour
3. Exercices encadrés en laboratoire

07 Évaluation des risques et rapport de test

1. Qualifier la gravité d'une vulnérabilité
2. Rédiger un rapport technique et une synthèse pour la direction

08 Remédiation et cas de synthèse

1. Recommandations de correction et suivi de leur mise en œuvre
2. Cas de synthèse en laboratoire