

Réaliser des tests d'intrusion (Sécurité Pentesting)

RS7394 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31006, 73054, 24293, 31045
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	27/11/2025
Date d'échéance	27/11/2028

Certificateur(s)

M2I · SIRET : 33354415300617

M2I · SIRET : 33354415300344

Partenaires habilités

6 organismes habilités, d'après la liste publiée par France compétences : 6 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
JEDHA	83872651100044	Former et organiser l'évaluation
M2I SCRIBTEL	39336786700214	Former et organiser l'évaluation
MICHEL KARTNER	79333268500023	Former et organiser l'évaluation
OO2	53157067900039	Former et organiser l'évaluation
STUDI	91114836900018	Former et organiser l'évaluation
SYSDREAM	45167612600043	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification « Réaliser des tests d'intrusion (Sécurité Pentesting) » s'adresse aux professionnels de la sécurité informatique souhaitant maîtriser l'ensemble des compétences nécessaires à la réalisation de tests d'intrusion.

Ces tests consistent à simuler les actions d'un attaquant potentiel afin d'évaluer le niveau de sécurité des réseaux, des systèmes et des environnements numériques d'une organisation. Ils incluent notamment l'analyse des flux réseau, des espaces de stockage et des vulnérabilités propres aux terminaux utilisés.

Dans un contexte marqué par l'intensification des cybermenaces, l'essor de l'intelligence artificielle, les impératifs croissants en matière de souveraineté numérique et la nécessité de conformité aux réglementations (RGPD, NIS2, etc.), cette certification répond à un besoin stratégique du marché. Elle permet de renforcer les compétences des professionnels face à la complexité croissante des environnements informatiques et à l'émergence de nouveaux vecteurs d'attaque, tout en intégrant des exigences éthiques, environnementales et réglementaires.

COMPÉTENCES ATTESTÉES

Définir les enjeux et contraintes du test d'intrusion, en tenant compte du cadre légal et réglementaire applicable, des principes éthiques, afin de définir les scénarios les plus probables ainsi que l'obtention du consentement légal.

Appliquer une méthodologie de test d'intrusion clair et reproductible, en documentant chaque étape du test, en privilégiant des outils et des pratiques alignés avec les principes d'éco-conception et de souveraineté numérique, afin de pouvoir restituer des éléments comparables dans leurs approches.

Concevoir et réaligner des outils d'intrusions, en intégrant des solutions d'IA, afin d'optimiser la détection des vulnérabilités répondre aux différents besoins d'un test d'intrusion.

Identifier les différentes vulnérabilités présentes, en réalisant les différentes phases des tests d'intrusions évoquées dans les enjeux initiaux afin de découvrir les points de faiblesses de l'organisation.

Remonter et restituer les différentes vulnérabilités identifiées, en élaborant un rapport structuré contenant un plan d'action et les mesures de sécurité afin de permettre à l'organisation de corriger ses failles.

Secteur d'activité et type d'emploi

RÈGLEMENTATIONS D'ACTIVITÉ

La réalisation de test d'intrusion (pentesting) n'est pas réglementée au sens strict. Toutefois, son exercice s'inscrit dans un cadre juridique exigeant, notamment en matière de cybersécurité, protection des données personnelles, éthique professionnelle et respect des systèmes d'information audités. Ces dimensions sont intégrées dans les compétences visées par la certification, et prises en compte à chaque étape du processus, à travers les méthodes, les livrables, et les pratiques associées à chaque bloc. Le respect des normes professionnelles, telles que celles de l'ANSSI, du RGPD ou du Code pénal (articles relatifs à l'accès non autorisé aux systèmes), constitue un socle incontournable de la pratique professionnelle visée.

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue

PRÉREQUIS À L'ENTRÉE EN FORMATION

Avoir des connaissances de base en réseaux : protocoles, adressage IP, routage ...

Avoir une compréhension du fonctionnement des systèmes Linux et/ou Windows : commandes de base, systèmes de fichiers

Être familier avec les systèmes de virtualisation comme VMWare, Hyper-V ou virtual Box

Avoir une appétence pour les grands domaines de la cybersécurité : sécurité des systèmes, des réseaux, des applications

COMPOSITION DU JURY — FORMATION CONTINUE

Le jury de certification est composé de deux professionnels experts en test d'intrusion (Pentesting), avec une expérience avérée de 3 ans, externes au certificateur.

Base légale

Date de décision	27/11/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	27/11/2028
Date de dernière délivrance possible	26/05/2029

Liens avec d'autres certifications

ANCIENNES VERSIONS

RS6092

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Réaliser des tests d'intrusion (Pentesting)

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/7394/>

Où se former

Formations référencées	12
Organismes	4
Régions couvertes	3
Prix indicatif	1 200 € – 11 200 €
Durée	150 – 190 h

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Entrées et sorties de formation

Entrées en formation	71
Parcours menés à terme	39
Taux d'achèvement	55 %
Période	01/2026 – 09/2026

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	102
Montant total engagé	166 733 €
Coût moyen par dossier	1 635 €
Durée moyenne	109 h
Période	12/2025 – 08/2026
France compétences	88 %
Reste à charge titulaire	6 %
OPCO	2 %
France Travail	2 %
Entreprise	2 %
Compte d'engagement citoyen	0 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.