

Réaliser des tests d'intrusion (Sécurité Pentesting)

RS6092 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	29/09/2022
Date d'échéance	29/09/2025

Certificateur(s)

M2I · SIRET : 33354415300344

Partenaires habilités

8 organismes habilités, d'après la liste publiée par France compétences : 8 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
CYBERINI	94818326400019	Former et organiser l'évaluation
EVOLUTION5	84999183100025	Former et organiser l'évaluation
JEDHA	83872651100044	Former et organiser l'évaluation
M2I SCRIBTEL	39336786700214	Former et organiser l'évaluation
M2I TECH	79504509500010	Former et organiser l'évaluation
MICHEL KARTNER	79333268500023	Former et organiser l'évaluation
OO2	53157067900039	Former et organiser l'évaluation
SCRIBTEL FORMATION	39336786700024	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 et permet d'acquérir toutes les compétences indispensables pour effectuer des tests qui consistent à examiner tous les réseaux et les systèmes informatiques en simulant les actions d'un intrus potentiel à l'intérieur de leur environnement de travail : analyse des flux, analyse des espaces de stockages, analyse de sécurité spécifique au terminal utilisé.

COMPÉTENCES ATTESTÉES

C.1.1 Définir les enjeux et contraintes du test d'intrusion dans l'objectif de définir les scénarios les plus probables ainsi que l'obtention du consentement légal.

C.1.2 Appliquer une méthodologie de test d'intrusion claire et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches.

C.1.3 Concevoir et réaligner des outils d'intrusion dans l'objectif de répondre aux différents besoins d'un test d'intrusion.

C.1.4 Identifier les différentes vulnérabilités présentes en réalisant les différentes phases des tests d'intrusion évoqués dans les enjeux initiaux dans le but de découvrir les points de faiblesses de l'organisation.

C.1.5 Remonter et restituer les différentes vulnérabilités identifiées ainsi qu'un plan d'actions contenant les mesures de sécurité permettant à l'organisation de corriger ses failles.

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue

PRÉREQUIS À L'ENTRÉE EN FORMATION

Prérequis : spécialiste en sécurité informatique, systèmes, réseaux et infrastructure globale. Avoir une appétence pour les différents systèmes d'exploitation.

Public cible : ingénieur cybersécurité, consultant sécurité, administrateur sécurité

COMPOSITION DU JURY — FORMATION CONTINUE

Le jury de certification est composé de deux personnes minimum, dont au moins deux professionnels experts en sécurité, avec une expérience avérée de 2 ans.

Base légale

Date de décision	29/09/2022
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	29/09/2025

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2021	107	—	—	—
2020	19	—	—	—

Liens avec d'autres certifications

ANCIENNES VERSIONS

RS2680

NOUVELLE(S) CERTIFICATION(S)

RS7394

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.m2iinformation.fr/m2i-pentesting/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/6092/>

Entrées et sorties de formation

Entrées en formation	236
Parcours menés à terme	230
Taux d'achèvement	97 %
Période	04/2023 – 01/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	258
Montant total engagé	591 349 €
Coût moyen par dossier	2 292 €
Durée moyenne	156 h
Période	03/2023 – 09/2025
France compétences	84 %
France Travail	7 %
Reste à charge titulaire	6 %
OPCO	3 %
Régions	0 %
Compte d'engagement citoyen	0 %
Entreprise	0 %

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