

Sécurité Pentesting

RS2680 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	31/12/2021

Certificateur(s)

M2I · SIRET : 33354415300344

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
M2I TECH	79504509500010	Former et organiser l'évaluation
SCRIBTEL FORMATION	39336786700024	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le certificat de compétences « Sécurité Pentesting » permet aux apprenants 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. La progression des candidats est consignée dans un livret d'évaluation individuel. Il contient les résultats des crédits acquis. Le candidat sera capable de :

- Définir la portée des tests,
- Réaliser les tests de pénétration,
- Etablir et diffuser les résultats d'analyse.

COMPÉTENCES ATTESTÉES

Définir les forces et faiblesses du système de sécurité en place.

Identifier les vulnérabilités.

Mesurer les impacts des menaces de sécurité.

Définir la portée des tests de pénétration.

Réaliser les tests de pénétration.

Etablir les résultats Pentesting.

Activité 1 : Utilisation des méthodologies de hacking

- Définir les enjeux et les règles de protection.
- Analyser les vulnérabilités
- Définir le degré de risque associé aux vulnérabilités.
- Exploiter les failles de sécurité.
- Conduire les méthodes de résolution des vulnérabilités découvertes.
- Identifier les aspects éthiques, économiques, juridiques et risques de la sécurité.

Activité 2 : Application des tests d'intrusion

- Analyser les besoins et les contraintes.
- Préparer le déroulement des tests d'intrusions.

- Mettre en place les maquettes, laboratoires et pilotes.
- Réaliser les tests d'intrusions.
- Déployer les solutions de scanner de vulnérabilités.
- Réaliser le suivi des vulnérabilités.
- Résoudre les incidents de sécurité.
- Préconiser les mesures de sécurité.
- Mettre en œuvre une veille sur les technologies de son domaine d'expertise.

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

- Ce Certificat est ouvert aux candidats justifiant d'un diplôme de niveau bac+3 dans le domaine de l'informatique ou d'une expérience professionnelle d'au moins deux ans dans un domaine compatible.
- Les candidats sont sélectionnés après un entretien et tests de positionnement.

Base légale

Date d'échéance de l'enregistrement 31/12/2021

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RS6092

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/2680/>

Entrées et sorties de formation

Entrées en formation	1
Parcours menés à terme	1
Taux d'achèvement	100 %
Période	06/2022

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

Demande CPF — formations engagées

Dossiers CPF engagés	174
Montant total engagé	174 167 €
Coût moyen par dossier	1 001 €
Durée moyenne	21 h
Période	01/2020 – 12/2021
France compétences	96 %
France Travail	2 %
Reste à charge titulaire	1 %

État	1 %
------	-----

Compte d'engagement citoyen	0 %
-----------------------------	-----

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