Sécurité Pentesting

CATEGORIE : C

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse : ▪ **Public et privé / tous les domaines d'activités**

Code(s) NAF : **62.02B**
Code(s) NSF : **326**
Code(s) ROME : **M1805**
Formacode : **31006**

Date de création de la certification : **20/06/2016**
Mots clés : **Hacking**, **Test d'intrusion**, **pentest**, **Cybersécurité**

Identification

Identifiant : **2680**
Version du : **08/04/2017**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :

- **Segments qui tirent la croissance d'ici 2020**
- **Les spécialistes de la cyber sécurité :**

Non formalisé :

- **L'ouverture électronique expose les entreprises à une nouvelle forme de délinquance et de vandalisme : la criminalité numérique. Pour se protéger et protéger leurs informations clés, les organisations mettent en œuvre une stratégie de sécurité en implémentant les derniers logiciels, périphériques et services pour prévenir les fraudes, les actes de vandalisme ou de sabotage et les attaques par déni de service. Il est donc essentiel de disposer de compétences pour vérifier que ces mesures de sécurité sont correctement implémentées et appliquées. Face aux menaces de plus en plus récurrentes, ces tests permettent aux entreprises d'expérimenter de**

manière concrète leur vulnérabilité aux attaques, mais sans en subir les conséquences."

Descriptif

Objectifs de l'habilitation/certification

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.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- non

Descriptif général des compétences constituant la certification

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.

Public visé par la certification

Tous publics

Modalités générales

Notre certification est fondée sur l'acquisition de compétences répondant aux besoins identifiés par les acteurs économiques. La durée recommandée est de 200 heures, les compétences qui conduisent à la certification sont construites de manière modulaire de façon à tenir compte des acquis des personnes. L'objectif est d'orienter le(s) candidat(s) vers une combinaison de modules, lui permettant d'obtenir, en fonction de ses acquis, la certification. La durée peut variée est établit en fonction des résultats des tests de positionnement permettant de créer des parcours adaptés. Une formation vise la polyvalence et l'ouverture à la vision de 360° exigée par le numérique. Toutes les compétences d'une session sont systématiquement évaluées tout au long de la formation.

Les étudiants sont accueillis tous les jours par un professionnel en activité consacrant une partie de son temps à la formation.

Un formateur référent est chargé de la sélection et du suivi des candidats, il est garant du respect du programme et supervise l'équipe des formateurs. Il complète le livret d'évaluation et prépare les candidats au certificat.

Des solutions de Blended learning (présentiel +e-learning) : Afin de nous adapter de façon constante aux évolutions technologiques innovantes, nous avons mis en place des solutions qui s'ajoutent au présentiel. Une plate-forme est disponible pour les étudiants et contient les supports de cours au format numérique et les tutoriaux. Ces modules permettent d'approfondir et de renforcer les connaissances acquises en présentiel.

Parce que nous sommes en relation permanente avec des professionnels, cela nous permet d'être en veille permanente et nous adaptons notre pédagogie à la réalité professionnelle. Notre approche reproduit les situations professionnelles et favorise les connaissances transférées. La mise en application de nos formations repose sur des cas concrets d'entreprise et mises en situation, qui poussent le stagiaire, non seulement à comprendre, mais à intégrer les points importants de son apprentissage.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

La certification « Sécurité Pentesting » constitue une validation fiable aux demandes actuelles du marché.
La certification permet l'acquisition de compétences permettant l'appropriation des démarches d'analyse des vulnérabilités afin d'évaluer les mesures de sécurité et l'infrastructure de sécurité par une approche proactive.
Elle témoigne d'un niveau opérationnel de l'expertise de son détenteur dans ce domaine. Le professionnel dispose alors d'un argument décisif pour l'obtention d'un emploi ou d'une mission.

Pour l'entité utilisatrice

Toutes les entreprises sont concernées par le piratage informatique ou l'incident de sécurité majeur. Ces compétences permettent de fournir des solutions pour aider les entreprises à se protéger dans le cyberespace.
L'examen certifiant est un outil fiable d'évaluation et de valorisation des compétences effectives des salariés. Inscrit dans un dispositif global de mise en situation d'entreprise, rendant ainsi, le candidat opérationnel et expert dans la spécialisation. Elle permet ainsi la montée en compétences des salariés et la possibilité d'une mobilité interne.

Evaluation / certification

Pré-requis

- 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.

Compétences évaluées

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.

Centre(s) de passage/certification

- Sur nos centres Paris/Ile de France : Rue de Picpus, Rue de Chaillot ou La Defense; et nos centres-régionaux- http://www.m2iformation.fr

- 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.

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

-

La validité est Permanente

Possibilité de certification partielle : non
Matérialisation officielle de la certification :
Certificat nominatif des compétences professionnelles acquises et décrites dans le référentiel de certification délivré par M2I Formation

Plus d'informations

Statistiques

Depuis le deuxieme semeste 2016, nous certifions une vingtaine de candidats. Nous avons une forte croissance du nombre d'inscrit depuis le début de l'année 2017.

Autres sources d'information

—