CYBERSECURITE / PENTEST

Soft Skills
Autonomie/ rigueur/ esprit analytique

Profil
Une appétence pour la cybersécurité et une capacite à résoudre des problèmes complexes.

Objectif

La formation vise à développer une expertise approfondie en cybersécurité.
L'objectif principal est d'équiper les apprenants avec des compétences avancées pour protéger les systèmes d'information contre diverses menaces numériques.
Le programme couvre une gamme étendue de sujets, allant des fondamentaux de la sécurité informatique, comme la compréhension des risques liés aux outils informatiques et la sécurisation de l'authentification, à des techniques plus avancées telles que le pentesting et la gestion de la sécurité réseau.
L'accent est également mis sur le développement des compétences pratiques en programmation (Python, SQL), cryptographie, et la gestion des systèmes sous Linux et Windows.
Cette approche holistique assure non seulement une compréhension technique approfondie mais aussi une conscience des implications juridiques et éthiques, préparant les apprenants à devenir des spécialistes complets en cybersécurité.

PROGRAMME

Maîtriser les fondements et les techniques élémentaires de la cybersécurité

Connaître les techniques de la cybersécurité basée sur le réseau

Appréhender les techniques d'attaque sur le web

Maîtriser les techniques d'hacking système

Maîtriser les techniques de cybersécurité : Pentest

FINANCEMENT : contactez-nous, nous vous aiderons dans vos démarches

Autofinancement

France Travail / AIF - Mon Compte Formation / CPF

Agefiph / Transition Pro

TARIF : 3 499 €

Public : Tout public

Délai d'accès : 4 semaines (selon le nombre de stagiaires)

Prérequis : aucun

Durée : 3 mois

Modalités d'organisation : en distanciel

Méthodes mobilisées :
Blended learning - Cours sur la plateforme dédiée
Accompagnement individuel par un formateur et un mentor en visioconférence
Exercices et quiz en ligne - Évaluations pour chaque bloc - Correction des exercices et évaluations avec le formateur dédié

Épreuve d'évaluation : Mise en situation professionnelle

L'épreuve est réalisée sur une durée de 4 heures. Chaque candidat se connecte individuellement à une Machine Virtuelle fournie et mise à disposition.
Chaque candidat devra sélectionner les outils et exploiter les différentes vulnérabilités pour effectuer un test d'intrusion sur la Machine Virtuelle mise à disposition.
Cette mise en situation fait l'objet :
- D'une présentation orale auprès de l'examinateur ;
- D'un rapport de pentest.
L'intégralité de l'examen doit faire l'objet d'un enregistrement vidéo à l'aide d'un logiciel dédié pour des raisons de transparence et de sécurité.
Evaluation orale :
Au cours ou à la suite de la mise en situation, l'examinateur questionne le candidat sur sa démarche et les méthodes utilisées selon la grille d'évaluation
Evaluation écrite :
La mise en situation fait l'objet d'un rapport de pentest évalué selon les critères du référentiel de certification par un évaluateur externe.

Modalités d'obtention de la certification :

La note globale est pondérée de la manière suivante :
➢ 70% pour l'évaluation du rapport de pentest, réparti comme suit :
- 50% : chacune des 5 compétences compte pour 10% et est évaluée selon les critères du référentiel. Pour chaque compétence, tous les points sont obtenus si tous les critères sont observés dans le rapport.
- 20% : qualité du rapport (Clarté et structure du rapport, Précision et exhaustivité des informations fournies, qualité des illustrations et des captures d'écran.)
➢ 30% pour l'évaluation orale

Pour valider la certification, la note globale obtenue doit être supérieure ou égale à 70/100.

Organisme certificateur : M2i
Formation certifiante inscrite au répertoire spécifique - Code RS 6092