Sécurité défensive

Cybersécurité - Devenez Pentester - Avec certification

20 jours (140h00) | ★★★★½ 4,6/5 | CYBER-PENTEST | Code RS ou RNCP : RS6092 | Certification Réaliser des tests d'intrusion (Sécurité Pentesting) (incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Formations Informatique › Cybersécurité › Sécurité défensive

Document mis à jour le 03/06/2024

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Enumérer les principales menaces et attaques courantes (DoS, DDoS, phishing...)
- Nommer les outils de pentesting couramment utilisés
- Décrire le cycle de vie d'une vulnérabilité
- Expliquer les différences entre les attaques sur le Web, les attaques sans fil et les attaques sur le réseau
- Démontrer l'utilisation d'outils pour découvrir des vulnérabilités
- Appliquer des techniques pour escalader des privilèges ou échapper à la détection
- Comparer et opposer différentes techniques d'attaque
- Analyser les résultats d'un scan pour identifier les vulnérabilités potentielles
- Concevoir un plan de test d'intrusion pour un système ou une application donnée
- Formuler des recommandations pour remédier aux vulnérabilités découvertes
- Evaluer la gravité et la criticité d'une vulnérabilité détectée
- Juger de la pertinence des mesures correctives proposées pour un problème donné
- Préparer et passer la certification "Réaliser des tests d'intrusion (Sécurité Pentesting)".

Compétences attestées par la certification

- 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
- Appliquer une méthodologie de test d'intrusion claire et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches
- Concevoir et réaligner des outils d'intrusion dans l'objectif de répondre aux différents besoins d'un test d'intrusion
- 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
- 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.

Lien pour visualiser le détail de la certification enregistrée au RS :
https://www.francecompetences.fr/recherche/rs/6092/

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir des connaissances de base en réseaux. Comprendre les concepts fondamentaux des réseaux informatiques, tels que les protocoles, l'adressage IP, les routages... Avoir des connaissances de base en systèmes. Avoir une compréhension des systèmes d'exploitation couramment utilisés, tels que Windows et Linux, y compris les commandes de base et les structures de fichiers. Connaître les plateformes de virtualisation. Etre familier avec les technologies de virtualisation, comme VMware ou VirtualBox, pour créer des environnements virtuels. Il est également nécessaire d'avoir des connaissances des grands domaines de la cybersécurité. Avoir une vue d'ensemble des différents domaines de la cybersécurité, tels que la sécurité des réseaux, la sécurité des systèmes, la sécurité des applications...

Public concerné

Techniciens systèmes et réseaux, administrateurs systèmes et réseaux, développeurs ayant une bonne connaissance des systèmes et réseaux, analystes SOC, RSSI...

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Préparation au hacking - Les connaissances de base (sur 2 jours)

- Réseaux
- Système
- Plateformes de virtualisations
- Les grands domaines de la cybersécurité
- Voyage dans le cyberespace (histoire)
- Les métiers de la cybersécurité
- Certifications en cybersécurité
- Organisation des acquis (Mind Map, Notion, start.me, Feed RSS...)
- Cybersécurité (liens, plateformes, analyse)
- Découvrir l'écosystème des tests d'intrusion (Pentest, Red Team, Blue Team, Purple Team...)
- Découvrir les principaux types d'attaques
- Les différentes phases d'une attaque

Techniques de hacking - Niveau 1 (sur 5 jours)

- Découvrir la notion de vulnérabilité
- Les standards de gestion de vulnérabilités
- CVE, CVSS, MITRE, CWE, NVD, IOC, OTX, Exploit, TTp
- Découvrir le framework ATT&CK
- OSINT (Open Source Intelligence)
- La récolte passive
- La récolte active
- L'exploitation

Tests d'intrusion sur les réseaux Wi-Fi (sur 2 jours)

- Introduction aux réseau sans fil
- Principes 802.11
- Menaces et attaques sur les réseaux sans fils
- Les protocoles de sécurité
- Architecture Wi-Fi sécurisée

Tests d'intrusion sur le Web (sur 3 jours)

- Top 10 OWASP
- Injection SQL et injection de code
- Brute force
- XXE
- Xss
- CSRF
- SSRF

Techniques de hacking - Niveau 2 (sur 5 jours)

- OSINT avancée
- Nmap et NSE
- Social engineering (phishing, smishing, usurpation de mail, fichiers piégés)
- Outils et framework d'obfuscation
- Framework C2
- Surface d'attaque de l'environnement Active Directory
- Modules de reconnaissances AD
- Techniques d'escalade de privilèges
- Persistance

Préparation à la certification (sur 2 jours)

- Méthode de rapport
- Méthode de rédaction
- Organisation de rapport
- Mise en situation

Passage de la certification (sur 1 jour)

- Modalités d'obtention de la certification "Réaliser des tests d'intrusion (Sécurité Pentesting)"
  - Le prix et le passage de la certification sont inclus dans cette formation
  - Une mise en situation professionnelle se déroulera sur 4h, à partir d'un besoin exprimé ou généré
  - Après cette dernière, le candidat présentera un rapport au jury qu'il défendra à l'oral durant un temps maximum d'1h30 (en détaillant la méthode, les outils choisis ainsi que les contre-mesures adéquates vis-à-vis des menaces et vulnérabilités identifiées lors de son pentest)
  - Une grille d'évaluation est complétée par le jury avec un score minimal de 70/100 pour la validation de l'ensemble des compétences de la certification

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- Au cours de la formation, par des études de cas et/ou des travaux pratiques
- En fin de formation, par le passage de la certification "Réaliser des tests d'intrusion (Sécurité Pentesting)", pour laquelle le jury de certification sera composé de deux personnes minimum, dont au moins deux professionnels experts en sécurité, avec une expérience avérée de 2 ans
- La certification se compose d'une réalisation d'un mini projet dans le cadre d'une étude de cas et d'une mise en situation professionnelle où il faudra sélectionner les outils et exploiter les différentes vulnérabilités pour effectuer un test d'intrusion.

Accessibilité de la formation

pagebreakavoidchecked="true";

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d'accès à la formation

pagebreakavoidchecked="true";

Les formations M2i sont disponibles selon les modalités proposées sur la page programme.
Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.