Sécurité offensive

Cours préparatoire aux techniques de hacking

2 jours (14h00) | ★★★★½ 4,6/5 | PREPA-HACK | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 23/05/2024.

Objectifs de formation

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

- Découvrir les notions de base en cybersécurité
- Expliquer le fonctionnement de la virtualisation (VMware)
- Mémoriser les bases d'utilisation des systèmes d'exploitation Windows et Linux
- Mettre en oeuvre les bases des protocoles réseaux (modèle OSI, TCP/IP, services, ports, Wireshark...)
- Découvrir la distribution orientée pentest Kali Linux
- Retenir l'essentiel pour suivre la formation SEC-HACK "Techniques de hacking - Niveau 1".

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 réseaux et système Linux de base.

Public concerné

Consultants cybersécurité, administrateurs et techniciens réseaux et systèmes, RSSI, DSI, chefs de projets cybersécurité, développeurs, responsables cybersécurité.

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

Jour 1

Les grands domaines de la cybersécurité

- Voyage dans le cyberespace (histoire)
- Les métiers de la cybersécurité
- Certifications en cybersécurité
- Organisation des acquis
  - MindMap
  - Notion
  - Start.me
  - Feed RSS...
- Découvrir les darknets
- 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

Découvrir les composants software et hardware d'un pentest

- Découvrir les plateformes de virtualisation
- Mise en place de l'hyperviseur VMware et prise en main
- Découvrir les distributions de pentest
- Prendre en main la distribution Kali

  - Navigation
  - Outils
  - Administration
  - Commandes de base
  - Réseaux
  - Meilleures pratiques
- Déploiement d'une plateforme de simulation pentest
- Découvrir le matériel du pentest physique :
  - Rubber Ducky
  - LAN Turtle
  - Wi-Fi Pineapple
  - O.MG Cable
  - Flipper Zero

Jour 2

Récapitulatif du jour précèdent

Les connaissances de base des réseaux

- Rappel sur le modèle OSI et TCP/IP
  - Fonctionnement des protocoles réseaux courants
  - ARP, ICMP, DHCP, HTTP(S), DNS, UDP...
- Apprendre à intercepter et analyser le trafic avec Wireshark
- Découvrir les options de base de Wireshark

Les standards de gestion de vulnérabilités

- Découvrir la notion de vulnérabilité
- Les standards de gestion de vulnérabilités
  - CVE, CVSS, MITRE, CWE, NVD, Exploit, CAPEC...
- Découvrir les groupes APT
- Découvrir le framework ATT&CK
  - Découvrir les notions de TTP et apprendre à utiliser le MITRE Navigator
- Préambule à la formation SEC-HACK "Techniques de hacking - Niveau 1"

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

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

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

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.