Sécurité offensive

Techniques de hacking - Niveau 2

5 jours (35h00) | SEC-HACK2 | 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 :

- Faire l'état des lieux des menaces récentes et des faiblesses d'infrastructure courantes
- Identifier et expérimenter des techniques de hacking avancées
- Reproduire des méthodes offensives dans la pratique.

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 suivi la formation SEC-HACK "Techniques de hacking - Niveau 1" ou avoir les connaissances équivalentes. Avoir des connaissances générales en système, réseau, développement et test d'intrusion sont un plus.

Public concerné

Etudiants, administrateurs système, consultants en sécurité de l'information.

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

- Récapitulatif des concepts de base de niveau 1
  - CVE, APT, IOC, OTX, CWE, Osint...
- Les méthodologies de pentest
- L'OSINT Investigator (mener l'enquête)

Jour 2

- Récapitulatif pratique (de niveau 1) des outils de scan
- Nmap et ses fonctionnalités avancées
- Scan de vulnérabilités
- Utilisation de NSE (Scripting Engine de Nmap)
- Utilisation de bases de données dans Metasploit
- Nessus et Metasploit

Jour 3

- Introduction aux techniques du "social engineering"
  - Phishing, smishing, usurpation de mail, fichiers piégés, QR code piégé, sites Web piégés
- Méthodes et outils d'obfuscation dans Metasploit
- Framework d'obfuscation
- Bypass Av et EDR (Endpoint Detection Response)
- Introduction aux frameworks C2
  - Covenant, Cobalt Strike, PoshC2
- Configuration et fonctionnement
- Mise en place de frameworks C2

Exemple de travaux pratiques (à titre indicatif)

- *Mise en pratique avec des exercices de "social engineering"*

Jour 4

- Introduction aux attaques ciblant les annuaires AD (Active Directory)
- Surface d'attaque de l'environnement AD
- Modules de reconnaissance
  - Enumération d'utilisateurs, groupes, domaines, GPO
- Techniques d'escalade de privilèges et de persistence
- Attaques contre les annuaires AD
  - Empoisonnement LLMNR (Link-Local Multicast Name Resolutio) et NBT-NS, attaque Kerberos, Golden Ticket

Exemples de travaux pratiques (à titre indicatif)

- *Mise en pratique avec des exercices d'utilisation (BloodHound, Zerologon, Golden Ticket, Silver Ticket, Kerberos)*

Jour 5

- Pentest dans un environnement d'entreprise
- Etude de cas de vulnérabilités potentielles du système d'information
- Corriger
- Récapitulatif
- Contre-mesures

Examen M2i (en option)

- Prévoir l'achat de l'examen en supplément
- L'examen (en français) sera passé le dernier jour, à l'issue de la formation et s'effectuera en ligne
- Il s'agit d'un QCM dont la durée moyenne est d'1h30 et dont le score obtenu attestera d'un niveau de compétence
- L'examen n'est pas éligible au CPF, mais permettra néanmoins de valider vos acquis

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 et/ou un examen M2i

Les + de la formation

Un examen M2i permettant de valider vos acquis à l'issue de la formation est disponible sur demande (coût : 120€).

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.