Techniques avancées

Attaque défense Wi-Fi

3 jours (21h00) | ⭐⭐⭐⭐⭐ 4,8/5 | WIFI | Évaluation qualitative de fin de stage | Formation délivrée en présentiel

Contenu mis à jour le 18/10/2024. Document téléchargé le 08/12/2024.

Objectifs de formation

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

- Décrire les types de réseaux Wi-Fi et les protocoles de sécurité courants
- Identifier les vulnérabilités courantes dans les réseaux Wi-Fi
- Mettre en pratique les méthodes d'attaque et de défense Wi-Fi
- Acquérir les compétences nécessaires pour configurer la sécurité sur un réseau Wi-Fi et détecter les intrusions.

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 des réseaux informatiques et des systèmes d'exploitation Windows ou Linux.

Public concerné

Professionnels de la sécurité informatique souhaitant améliorer leurs compétences en matière de sécurité Wi-Fi, administrateurs réseau ou toute personne souhaitant comprendre les risques liés aux réseaux Wi-Fi et les méthodes pour les protéger.

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

Introduction à la sécurité Wi-Fi

- Types de réseaux Wi-Fi
  - Infrastructure
  - Ad-hoc...
- Protocoles de sécurité courants
  - WEP
  - WPA
  - WPA2
- Vulnérabilités courantes
  - Faiblesses de la clé
  - Attaques de désauthentification
- Outils de reconnaissance de réseau

Exemples de travaux pratiques (à titre indicatif)

- *Utilisation d'outils de reconnaissance de réseaux tels qu'Airodump-ng ou Kismet pour scanner les réseaux Wi-Fi disponibles*
- *Utilisation d'outils pour tester les vulnérabilités identifiées (par exemple : Aircrack-ng, inssider)*

Jour 2

Attaques Wi-Fi

- Méthodes d'attaques Wi-Fi
  - Cracking de mot de passe
  - Injection de paquets
  - Attaques de désauthentification
  - PMKID (Pairwise Master Key Identifier)
- Outils d'attaques courants
  - Aircrack-ng
  - Aireplay-ng
  - Airgedon

Exemples de travaux pratiques (à titre indicatif)

- *Utilisation d'outils pour mettre en pratique les différentes méthodes d'attaques sur des réseaux Wi-Fi vulnérables*
- *Utilisation de scénarios d'attaque pour simuler des situations réelles*

Jour 3

Défense Wi-Fi

- Meilleures pratiques pour protéger les réseaux Wi-Fi
  - Configuration de la sécurité
  - Surveillance
  - Détection d'intrusion
- Outils de sécurité courants
  - Wireshark
  - WaIDpS
  - Chellam

Exemples de travaux pratiques (à titre indicatif)

- *Configuration de la sécurité sur un réseau Wi-Fi (par exemple : utilisation de WPA2-AES)*
- *Utilisation d'outils pour détecter les intrusions (par exemple : WaIDpS pour détecter des attaques de désauthentification)*
- *Mise en place de contre-mesures pour se protéger contre les attaques Wi-Fi*
- *Utilisation de scénarios de défense pour simuler des situations réelles*

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

Les + de la formation

Les exercices incluront des activités pratiques telles que la configuration de la sécurité sur un réseau Wi-Fi, la détection d'intrusion, la mise en place de contre-mesures pour se protéger contre les attaques Wi-Fi, la réalisation de scénarios d'attaque / défense.

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page Accueil PSH.

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.