

## Techniques de hacking – Niveau intermédiaire

5 jours (35 heures)

Expertise

Présentiel ou classe à distance

à partir de

**3 925 € HT** par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 04/10/2026.

### Objectifs

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

- Utiliser des outils de pentesting et des techniques d'exploitation
- Mettre en oeuvre des méthodologies et techniques d'attaque réseau plus avancées, incluant l'Active Directory et le social engineering
- Déterminer les contre-mesures avancées pour protéger le SI.

Les compétences visées par cette formation font l'objet d'une évaluation.

### À qui s'adresse cette formation ?

Professionnels de la sécurité informatique ayant une première expérience en pentesting, administrateurs système et réseau souhaitant approfondir leurs connaissances en sécurité, consultants en sécurité avancée.

#### Prérequis

Avoir suivi la formation SEC-HACK "Techniques de hacking – Les fondamentaux" ou avoir les connaissances équivalentes. Savoir maîtriser les concepts de base de la sécurité des réseaux et des systèmes d'information.

# Programme

## 1 Pendant votre formation

### Techniques de hacking – Niveau intermédiaire

Jour 1 – Matin

#### Récapitulatif et méthodologies avancées de pentesting

- Récapitulatif des bases vues en niveau 1
- Méthodologies avancées
  - PTES
  - OSSTMM
  - OWASP
- OSINT avancée

Jour 1 – Après-midi

*Exemple de travaux pratiques (à titre indicatif)*

- Application des méthodologies avancées d'OSINT

Jour 2 – Matin

#### Outils et techniques avancés de reconnaissance et scan

- Utilisation avancée de Nmap
  - Détection furtive
  - Scripts NSE personnalisés
- Introduction aux bases de données d'exploits
  - Metasploit
  - Exploit-db

Jour 2 – Après-midi

*Exemple de travaux pratiques (à titre indicatif)*

- Scan avancé de réseaux et bases de données d'exploits

Jour 3 – Matin

#### Introduction aux attaques ciblant Active Directory (AD) et mouvements latéraux

- Introduction aux attaques AD
  - Kerberos
  - LLMNR / NBT-NS Poisoning
- Techniques de mouvement latéral avec PowerShell (ex PowerView)

Jour 3 – Après-midi

*Exemple de travaux pratiques (à titre indicatif)*

- *Attaques sur une structure AD fictive*

Jour 4 – Matin

### **Social engineering et contournement d'anti-virus**

- Techniques d'ingénierie sociale
  - Phishing
  - Smishing
  - Qshing
- Introduction aux frameworks de command-and-control (C2) open source et contournement d'anti-virus

Jour 4 – Après-midi

*Exemples de travaux pratiques (à titre indicatif)*

- *Mise en place d'un serveur C2 et contournement d'anti-virus*

Jour 5 – Matin

### **Documentation et contre-mesures avancées**

- Documentation avancée des résultats d'un test d'intrusion
- Mise en place de contre-mesures avancées

Jour 5 – Après-midi

*Exemples de travaux pratiques (à titre indicatif)*

- *Documentation et élaboration de contre-mesures spécifiques*

## **Financement**

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

**Nous contacter pour en savoir plus →**

## Modalités 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

### Accessibilité aux personnes en situation de handicap

## Détails de la session

Du 30 novembre 2026 au 4 décembre 2026 (5 jours / 35 heures)

Grenoble

Du 30 novembre 2026 au 4 décembre 2026

Grenoble

- 30 novembre 2026 ..... 9h00 – 15h00
- 1 décembre 2026 ..... 9h00 – 15h00
- 2 décembre 2026 ..... 9h00 – 15h00
- 3 décembre 2026 ..... 9h00 – 15h00
- 4 décembre 2026 ..... 9h00 – 15h00