

Techniques de hacking – Les fondamentaux

5 jours (35 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

3 675 € HT par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 30/09/2026. Document téléchargé le 02/10/2026.

Formation Techniques de hacking et contre-mesures | Certification TOSA | Eligible au CPF | Détectez les fragilités d'un système par la connaissance des différentes cibles d'un piratage. 35 centres partout en France. Formation en présentiel

Objectifs

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

- Identifier les bases du hacking éthique et les concepts fondamentaux de la sécurité des systèmes d'information
- Déterminer les différentes étapes d'un test de pénétration de base
- Utiliser les principaux outils de reconnaissance et de collecte d'information
- Reconnaître les contre-mesures basiques pour protéger un SI.

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

À qui s'adresse cette formation ?

Professionnels de la sécurité informatique, administrateurs système et réseau, consultants en sécurité et/ou toute personne souhaitant débiter dans le domaine du hacking éthique et des tests d'intrusion.

Prérequis

Avoir des connaissances de base en réseaux et systèmes d'exploitation et des notions élémentaires de sécurité informatique.

Programme

1 Pendant votre formation

Techniques de hacking – Les fondamentaux

Jour 1 – Matin

Introduction et bases du pentesting

- Introduction au hacking éthique et à la cybersécurité
- Cadre juridique et éthique du hacking
- Les phases du test d'intrusion
 - Reconnaissance
 - Scan
 - Exploitation
 - Post-exploitation

Jour 1 – Après-midi

Introduction et bases du pentesting – Suite

- Introduction aux outils de collecte d'information
 - Google Hacking
 - Maltego
 - OSINT

Exemple de travaux pratiques (à titre indicatif)

- Réalisation d'une reconnaissance passive sur une cible fictive

Jour 2 – Matin

Reconnaissance active et scan de vulnérabilités

- Techniques de reconnaissance active : scan réseau et scan de ports avec Nmap
- Utilisation avancée de Nmap et des scripts NSE

Jour 2 – Après-midi

Reconnaissance active et scan de vulnérabilités – Suite

- Découverte des scanners de vulnérabilités
 - OpenVAS
 - Nikto pour le Web

Exemples de travaux pratiques (à titre indicatif)

- Identification et analyse de vulnérabilités

Jour 3 – Matin

Attaques réseau et sécurité des connexions

- Introduction au Man-in-the-Middle (MITM) et attaques réseau basiques (ARP spoofing, DNS spoofing)
- Introduction à l'outil Ettercap pour les attaques MITM

Jour 3 – Après-midi

Attaques réseau et sécurité des connexions – Suite

- Contre-mesures pour sécuriser le réseau local

Exemple de travaux pratiques (à titre indicatif)

- Exécution d'une attaque MITM

Jour 4 – Matin

Exploitation des vulnérabilités et bases de Metasploit

- Introduction à Metasploit et aux payloads
 - Création de shellcodes basiques
- Exploitation de vulnérabilités simples
 - Failles basiques

Jour 4 – Après-midi

Exemple de travaux pratiques (à titre indicatif)

- Exploitation de vulnérabilités basiques sur des machines virtuelles cibles

Jour 5 – Matin

Post-exploitation et documentation

- Introduction à la post-exploitation : collecte d'informations sur la cible
- Techniques de base pour maintenir l'accès
 - Backdoors simples

Jour 5 – Après-midi

Post-exploitation et documentation – Suite

- Techniques de base pour l'élévation de privilèges
- Recommandations de sécurité
 - Les meilleures pratiques et normes
 - Retour d'expérience
- Discussion sur les tendances de cybersécurité et l'évolution dans ce domaine

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 4 octobre 2027 au 8 octobre 2027 (5 jours / 35 heures)

Nancy

Du 4 octobre 2027 au 8 octobre 2027

Nancy

- 4 octobre 2027 9h00 – 15h00
- 5 octobre 2027 9h00 – 15h00
- 6 octobre 2027 9h00 – 15h00
- 7 octobre 2027 9h00 – 15h00
- 8 octobre 2027 9h00 – 15h00