

Sessions garanties disponibles

Formation Tests d'intrusion

Réf. SF33586

Effectuez des tests d'intrusion efficaces, identifiez les vulnérabilités et atténuez les risques de sécurité grâce à notre formation complète !

4 j Durée	3 200 € HT Inter / participant	8 200 € HT Intra (≤12 pers.)	13 Sessions à venir
--------------	-----------------------------------	---------------------------------	------------------------

Objectifs pédagogiques

- ✓ Identifier et catégoriser les différents types de vulnérabilités dans les systèmes informatiques.
- ✓ Appliquer efficacement les méthodologies de test d'intrusion standard de l'industrie.
- ✓ Effectuer une reconnaissance approfondie à l'aide de l'OSINT et d'autres techniques.
- ✓ Utiliser divers outils et cadres pour le balayage et l'analyse des réseaux.
- ✓ Exécuter des exploits pour évaluer les vulnérabilités des systèmes.
- ✓ Mettre en œuvre des mesures de post-exploitation pour maintenir l'accès et extraire les données en toute sécurité.

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux,
Développeurs, Testeurs logiciels

Prérequis Solide compréhension des réseaux et des systèmes d'exploitation, familiarité avec les concepts de base de la cybersécurité et la ligne de commande Linux.

Programme détaillé

Introduction aux tests d'intrusion

Définition des tests d'intrusion et de leur utilité en matière de cybersécurité
Aperçu des phases et des méthodologies des tests d'intrusion
Considérations éthiques et implications juridiques
Introduction aux outils et environnements utilisés dans les tests d'intrusion

Activités pratiques :

Mise en place d'un laboratoire virtuel de tests d'intrusion pour simuler des scénarios réels.

Reconnaissance et collecte d'informations

Techniques de renseignement de source ouverte (OSINT)
Méthodes de reconnaissance active et passive
Analyse et énumération de réseaux à l'aide de Nmap
Identification des services et extraction d'informations

Activités pratiques :

Effectuer un balayage du réseau pour identifier les hôtes actifs et les ports ouverts à l'aide de Nmap.

Identification et analyse des vulnérabilités

vulnérabilités

Types courants de vulnérabilités dans les systèmes informatiques
Outils et techniques d'évaluation des vulnérabilités
Interprétation des rapports des scanners de vulnérabilité
Analyse des configurations des systèmes pour détecter les faiblesses potentielles

Activités pratiques :

Utiliser un scanner de vulnérabilité pour identifier les mauvaises configurations et les vulnérabilités connues.

Techniques d'exploitation

Introduction aux cadres d'exploitation comme Metasploit
Création et déploiement d'exploits pour diverses vulnérabilités
Techniques d'escalade des privilèges
Éviter la détection lors de l'exploitation

Activités pratiques :

Utiliser Metasploit pour déployer un exploit contre un service vulnérable.

Stratégies post-exploitation

Maintien d'un accès persistant aux systèmes compromis
Méthodes d'exfiltration des données et évitement de la détection
Techniques de pivotement pour explorer les réseaux internes
Effacer les traces et améliorer la sécurité opérationnelle

Activités pratiques :

Extraire des données sensibles d'un serveur compromis en évitant la détection.

Rapports et documentation

Créer des rapports de tests d'intrusion efficaces
Documenter les résultats et fournir des recommandations exploitables
Communiquer les résultats aux parties prenantes techniques et non techniques
Assurer la conformité avec les normes et les meilleures pratiques de l'industrie

Activités pratiques :

Rédiger un rapport de test d'intrusion résumant les résultats et suggérant des mesures correctives.

Prochaines sessions

DATE	LIEU	STATUT
30/11/2026	à distance	Sur confirmation
08/03/2027	Lyon	Sur confirmation
08/03/2027	Grenoble	Sur confirmation
08/03/2027	Nantes	Sur confirmation
08/03/2027	à distance	Sur confirmation
15/06/2027	Aix-en-Provence	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Amaury P. — Formateur Sécurité Offensive & Red Team

Amaury intervient sur des formations portant sur la sécurité offensive, le Red Team et le pentest. Parmi les formations qui lui sont confiées figurent notamment « Ethical Hacking » et...

Ils nous font confiance

Cette année notre filière Cybersécurité et Protection des Données a accompagné plus de 69 entreprises dont :

AVEM MÉTROPOLE DE LYON ACTIMAGE CONSULTING SAS ADISTA ADVENTIEL AIGA ALCYOR ALDORIA ALSTOM ALTEN SA +59 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com