

Sessions garanties disponibles

Formation Python pour les tests d'intrusion

Réf. SF33607

Utilisez efficacement Python pour le pentest grâce à notre formation de 4 jours !

4 j Durée	2 800 € HT Inter / participant	7 800 € HT Intra (≤12 pers.)	1 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Comprendre le rôle de Python dans les tests de pénétration et ses avantages par rapport à d'autres langages de programmation
- ✓ Décrire les concepts fondamentaux de Python et la manière dont ils s'appliquent aux tests d'intrusion
- ✓ Utiliser des bibliothèques et des outils Python spécifiques aux tests de pénétration
- ✓ Créer et exécuter des scripts Python personnalisés pour divers scénarios de pentest
- ✓ Interpréter les résultats des tests de pénétration basés sur Python pour identifier les faiblesses de sécurité

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux,
Développeurs

Prérequis Connaissances de base en programmation Python (variables, boucles, fonctions, etc.), familiarité avec les concepts et les protocoles réseaux, capacité à travailler dans un environnement ligne de commande.

Programme détaillé

Introduction à la formation Python pour les tests d'intrusion

Vue d'ensemble du rôle de Python dans la cybersécurité
Avantages de l'utilisation de Python pour les tests d'intrusion
Mise en place de l'environnement de développement :

- Installation de Python et des bibliothèques appropriées
- Introduction aux IDE et aux éditeurs de texte

Rappel des notions de base de Python :

- Types de données, variables et opérateurs
- Structures de contrôle : boucles et conditionnelles
- Fonctions et modules

Activités pratiques :

Mise en place d'un environnement de développement Python, écrire des scripts Python simples pour automatiser des tâches.

Scanning réseau et phase d'énumération

Comprendre les techniques d'analyse réseau :

- Ping sweep et scanning des ports
- Détection des services et des versions

Bibliothèques Python pour l'analyse de réseaux : scapy, socket, nmap...
Développement de scripts d'analyse personnalisés
Techniques d'énumérations : utilisateurs, services, SMB...

Activités pratiques :

Écriture d'un script pour effectuer un scanning réseau de base, création d'un scan de ports personnalisé à l'aide de Python.

Evaluation des vulnérabilités

Identifier les vulnérabilités courantes :

- Top 10 de l'OWASP
- Dictionnaire CVE (Common Vulnerabilities and Exposures)

Exemples d'outils Python pour l'évaluation des vulnérabilités :

- requests et BeautifulSoup pour le scraping et l'analyse de sites web
- paramiko pour l'interaction SSH

Automatisation des analyses de vulnérabilité, intégration avec des outils existants comme OpenVAS et Nessus

Activités pratiques :

Écriture d'un script Python pour rechercher des vulnérabilités connues sur un site web, automatiser un scan de vulnérabilité et analyser les résultats.

Techniques d'exploitation

Comprendre les frameworks d'exploitation

Intégration d'outils comme Metasploit avec Python

Écrire des scripts d'exploitation personnalisés en Python :

- Buffer overflow exploits
- Web application exploits

Utiliser Python pour les attaques d'ingénierie sociale :

- Email spoofing
- Simulations de phishing

Activités pratiques :

Développement d'un script Python pour exploiter une vulnérabilité buffer overflow, écriture d'un script générateur d'e-mails de phishing.

Post-exploitation et reporting

Maintien de l'accès à l'aide de backdoors et payloads :

- Reverse shells
- Mécanismes de persistance

Techniques d'exfiltration de données à l'aide de Python

Générer des rapports de tests de pénétration :

- Automatisation de la génération de rapports
- Formatage et exportation des résultats

Activités pratiques :

Création d'un payload de type « reverse shell » avec Python, écrire un script pour automatiser la génération d'un rapport de test de pénétration.

Projet recap

Intégrer tous les concepts appris :

- Conception d'un script de test de pénétration complet
 - Réalisation d'un test de pénétration complet sur un réseau simulé
- Présentation et feedback des pairs sur les projets de fin de formation

Prochaines sessions

DATE	LIEU	STATUT
16/11/2026	à distance	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

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 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

Pauline S. — Formatrice

Pauline intervient notamment sur le Digital Workplace et Microsoft 365, ainsi que sur la gestion de projet et les certifications associées. Son activité de formation remonte à 2005, soit plus...

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