Python pour tests d'intrusion

Code : DEV-PYTHON-330 Durée : 3 jours (21 heures)

Public visé

Professionnels de la cybersécurité et développeurs voulant acquérir une expertise sécurité.

Prérequis

Connaissances fondamentales en informatique et cybersécurité. Connaissance préalable de Python nécessaire.

Objectifs pédagogiques

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

- Exécuter les opérations Python fondamentales (I/O fichiers, sockets réseau)
- Analyser et interagir avec des systèmes/réseaux
- Exploiter des vulnérabilités
- Implémenter des techniques de post-exploitation
- Créer des scripts de tests d'intrusion automatisés

Programme

Jour 1

Fondamentaux Python pour la sécurité

- Configuration de l'environnement
- Variables, types, structures de contrôle
- Fonctions

Jour 2

Analyse réseau et exploitation

- Opérations fichiers et sockets
- Analyse de paquets réseau
- Techniques d'exploitation
- Exécution de commandes à distance

Jour 3

Post-exploitation et automatisation

- Post-exploitation et persistance
- Automatisation
- Développement de scripts complets de pentest