

Python pour test d'intrusion

3 jours - 21 heures

Code formation : ADHSYS0726



adhara.fr

Objectifs

Acquérir les compétences nécessaires en scripting pour créer vos propres outils en Python pour un test d'intrusion.

Participants

Tout pentester, développeur et administrateur.

Prérequis

Disposer des connaissances généralistes en programmation.

Ouverture vers l'Intelligence Artificielle

Le formateur proposera, lorsque pertinent, un éclairage sur les usages complémentaires de l'intelligence artificielle en lien avec le programme : automatisation de tâches, assistance à l'analyse et à la création de contenus, optimisation des processus ou encore support à la prise de décision. Ces apports permettront d'illustrer de nouvelles pratiques tout en sensibilisant aux bonnes règles d'utilisation responsable (sécurité, fiabilité des résultats, respect des données).

Programme

Introduction

Introduction à Python et à la Cybersécurité
Environnement Python et création du lab
Rappel des bases Python et différentes API (Application Program Interface)
Monter un exécutable en Python

Réseau

Gestion des sockets
Création d'un scan de ports
Introduction à la bibliothèque Scapy
Mise en place d'ARP poisoning (MITM) avec Scapy
Subprocess : Reverse Shell

Système

Win32Clipboard : manipuler le presse-papier
Programme auto-répliquant
Cryptographie : Ransomware
Détection et protection en temps réel d'un ransomware
Fonctionnement d'un Keylogger
Exfiltration (type et protocole)
Exfiltration FTP : screenshots

Web

Introduction aux bibliothèques Web (BeautifulSoup et Request)
Protocole HTTP et fonctionnement
Requêtes HTTP(s)
BeautifulSoup : Crawler
Injection dans le DOM
MITMproxy : Frame Injection
API Web : Shodan

Remarques

Python pour test d'intrusion

3 jours - 21 heures

Code formation : ADHSYS0726



adhara.fr

Pédagogie

La pédagogie est basée sur le principe de la dynamique de groupe avec alternance d'apports théoriques, de phases de réflexion collectives et individuelles, d'exercices, d'études de cas et de mises en situations observées. Formation / Action participative et interactive : les participants sont acteurs de leur formation notamment lors des mises en situation car ils s'appuient sur leurs connaissances, les expériences et mettront en œuvre les nouveaux outils présentés au cours de la session.

Public Visé

Collaborateurs - Développer ses compétences, s'affirmer comme expert dans son domaine, sécuriser son parcours professionnel ;
Entreprises ou organisations - Accélérer les évolutions de carrière des collaborateurs, augmenter l'efficacité et l'employabilité des équipes... ;
Demandeur d'emploi - Développer son employabilité, favoriser sa transition professionnelle...

Profil de l'intervenant

Consultant-formateur expert. Suivi des compétences techniques et pédagogiques assuré par nos services.

Moyens techniques

Encadrement complet des stagiaires durant la formation. Espace d'accueil, configuration technique des salles et matériel pédagogique dédié pour les formations en centre. Remise d'une documentation pédagogique papier ou numérique à échéance de la formation.

Méthodes d'évaluation des acquis

Un contact téléphonique est systématiquement établi avec le stagiaire ou la personne chargée de son inscription afin de définir le positionnement. Si besoin, un questionnaire est adressé pour valider les prérequis en correspondance et obtenir toute précision nécessaire permettant l'adaptation de l'action. Durant la formation, des exercices individuels et collectifs sont proposés pour évaluer et valider les acquis du stagiaire. La feuille d'émargement signée par demi-journée ainsi que l'évaluation des acquis sont adressées avec la facture.