PYTHON POUR LE PENTEST

Développement et exploitation avec Python pour le Pentest

Code : PYTPEN

Cette formation destinée aux personnes ayant déjà une connaissance basique du langage Python, arbore les di!érents modules et cas d'utilisation de Python lors de tests d'intrusions.
Nous verrons de nombreuses problématiques rencontrées lors d'audits et les solutions pouvant être mises en place rapidement grâce au scripting Python afin d'automatiser les tâches complexes et spécifiques

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation grâce à 80% d'exercices pratiques et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.

JOUR 1

Python pour le HTTP, requests
- Développement d'un système de recherche exhaustive
- Contournement de captcha

Développement d'un module Python BurpSuite
- Introduction à BurpSuite
- Développement d'un module de détection passif de Web Application Firewalls

Exploitation d'une injection SQL en aveugle
- Extraction bit à bit et analyse comportementale

JOUR 2

Python et l'altération http
- Introduction à MITMProxy
- Développement d'un module «SSL Striping»

Python et le forensics
- Volatility
- Hachoir
- Network Forensics avec Scapy

JOUR 3

Le C et Python, Cython
- ctypes
- Développement d'un module Cython Antivirus et Backdoors

Antivirus et Backdoors
- Shellcodes
- Création d'une porte dérobée avancée

JOUR 4

Chaîne d'exploitation
- Exploitation de multiples vulnérabilités
- Création d'un exploit complet (POC)

TP Final
- Capture the Flag

FORMATION SUR DEVIS

OBJECTIFS

- Faciliter le développement d'exploits en Python
- Automatiser le traitement de tâches et automatiser les exploitations
- Contourner les solutions de sécurité
- Interfacer différents langages avec Python

INFORMATIONS GÉNÉRALES

Code : PYTPEN
Durée : 4 jours
Prix : Sur devis
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- RSSI
- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux

PRÉ-REQUIS

- Connaissances en Python

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne / Internet
- Machine virtuelles Windows/Linux