Python pour le Pentest

Cours Pratique de 4 jours - 28h
Réf : PYH - Prix 2024 : 2 390€ HT

Cette formation destinée aux personnes ayant déjà une connaissance basique du langage Python arbore les différents modules et cas d'utilisations de Python lors de tests d'intrusions.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

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

MÉTHODES PÉDAGOGIQUES

L'évaluation des acquis se fait tout au long de la session au travers des multiples exercices à réaliser (50 à 70% du temps).

LE PROGRAMME

dernière mise à jour : 10/2020

1) Python pour le HTTP, requests

- Développement d'un système de recherche exhaustive.
- Contournement de captcha.

2) Développement d'un module Python BurpSuite

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

3) Exploitation d'une injection SQL en aveugle

- Extraction bit à bit et analyse comportementale.

4) Introduction aux tâches distribuées

- Introduction à l'attaque Slowloris.
- Développement d'un exploit Slowloris distribué.

5) Python et l'altération HTTP

- Introduction à MITMProxy.
- Développement d'un module "SSL Striping".

6) Python et le forensics

- Volatility.
- Hachoir.
- Network Forensics avec Scapy.

7) Le C et Python, Cython

- ctypes.
- Développement d'un module Cython Antivirus et backdoors.

PARTICIPANTS

RSSI, consultants en sécurité, ingénieurs et techniciens, administrateurs systèmes et réseaux.

PRÉREQUIS

Connaissances en Python.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

8) Antivirus et backdoors

- Shellcodes.
- Création d'une porte dérobée avancée.

9) Chaîne d'exploitation

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

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 09 juil., 22 oct.	2024 : 02 juil., 15 oct.