Publication date : 06/13/2024

Course : Python for Pentest

Practical course - 4d - 28h00 - Ref. PYH
Price : 2470 CHF E.T.

3,8 / 5

This course, designed for people with a basic knowledge of the Python language, covers the various modules and uses of Python in intrusion testing.

Teaching objectives

At the end of the training, the participant will be able to:

- Facilitating the development of exploits in Python
- Automate task processing and operations
- Bypassing security solutions
- Interfacing different languages with Python

Intended audience

CISOs, security consultants, engineers and technicians, system and network administrators.

Prerequisites

Knowledge of Python.

Practical details

Teaching methods

Assessment of learning is carried out throughout the session through a series of exercises (50-70% of the time).

Course schedule

1 Python for HTTP, requests

- Development of an exhaustive search system.
- Captcha bypass.

2 Development of a BurpSuite Python module

- Introduction to BurpSuite.
- Development of a passive detection module for Web Application Firewalls.

PARTICIPANTS

CISOs, security consultants, engineers and technicians, system and network administrators.

PREREQUISITES

Knowledge of Python.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

3 Exploiting a blind SQL injection

- Bit-by-bit extraction and behavioral analysis.

4 Introduction to distributed tasks

- Introduction to the Slowloris attack.
- Development of a distributed Slowloris exploit.

5 Python and HTTP tampering

- Introduction to MITMProxy.
- Development of a "SSL Striping" module.

6 Python and forensics

- Volatility.
- Mincer.
- Network Forensics with Scapy.

7 C and Python, Cython

- ctypes.
- Development of a Cython Antivirus and backdoors module.

8 Antivirus and backdoors

- Shellcodes.
- Creation of an advanced backdoor.

9 Operating chain

- Exploitation of multiple vulnerabilities.
- Creation of a complete exploit (POC).

Dates and locations

REMOTE CLASS
2026 : 3 Mar., 23 June, 22 Sep.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.