

Python Security | Introduction to Python Programming for Security Analysts & Professionals - **TTPS4894**

Implement Better Defenses in Python | Python Essentials, File Operations, Binary Data, Networking Services, Python Security & More

Duration: 4 Days

Skill Level: Introductory

Available Format: Instructor-Led Online; Instructor-Led, Onsite In Person ; Blended; On Public Schedule

Geared for experienced security professionals new to Python, Python Programming for Security Analysts & Professionals is practical, hands-on Python training course that leads the student from the basics of writing and running Python scripts to more advanced features such as file operations, regular expressions, working with binary data, and using the extensive functionality of Python modules.

What You'll Learn

Overview

Geared for experienced security professionals new to Python, Python Programming for Security Analysts & Professionals is practical, hands-on Python training course that leads the student from the basics of writing and running Python scripts to more advanced features such as file operations, regular expressions, working with binary data, and using the extensive functionality of Python modules. Extra emphasis is placed on features unique to Python, such as tuples, array slices, and output formatting.

This course is tailored specifically for Security Analysts and others who wish to use Python functionality for security-related tasks such as log manipulation or forensics.

This course is essential for security professionals that are performing security reviews and audits of Python applications or are supporting development teams in implementing better defenses in Python.

Objectives

This course combines expert lecture, real-world demonstrations and group discussions with machine-based practical labs and exercises. Throughout the hands-on course students will learn to write essential Python scripts using the most current and efficient skills and techniques.

Working in a hands-on learning environment, guided by our expert team, attendees will learn to:

- Create working Python scripts following best practices
- Use python data types appropriately
- Read and write files with both text and binary data
- Search and replace text with regular expressions
- Get familiar with the standard library and its work-saving modules
- Use lesser known but powerful Python data types
- Create "real-world", professional Python applications
- Work with dates, times, and calendars
- Know when to use collections such as lists, dictionaries, and sets
- Understand Pythonic features such as comprehensions and iterators
- Write robust code using exception handling
- Write Secure Python Applications
- Perform Log File Analysis
- Work with Security Filters, Packet Analysis and related Analytics
- Time Permitting / Bonus Content: Working with RESTful Services and OWASP Top Ten Review

Need different skills or topics? If your team requires different topics or tools, additional skills or custom approach, this course may be further adjusted to accommodate. We offer additional python, security, web development, data science, machine learning and other related topics that may be blended with this course for a

track that best suits your goals. Our team will collaborate with you to target the course to focus on your specific learning objectives.

Audience

This course is tailored specifically for Security Analysts and others new to Python, who wish to learn and use Python functionality for security-related tasks such as log manipulation or forensics. Students are required to have some basic programming experience and exposure prior to attending this course. Students should have basic development experience in any programming language, along with a working, user-level knowledge of Unix/Linux, Mac, or Windows.

Pre-Requisites

Students are required to have some basic programming experience and exposure prior to attending this course. Students should have basic development experience in any programming language, along with a working, user-level knowledge of Unix/Linux, Mac, or Windows.

Agenda

Please note that this list of topics is based on our standard course offering, evolved from typical industry uses and trends. We will work with you to tune this course and level of coverage to target the skills you need most. Course agenda, topics and labs are subject to adjust during live delivery in response to student skill level, interests and participation.

An Overview of Python

- What is python?
- Python Timeline
- Advantages/Disadvantages of Python
- Getting help with pydoc

The Python Environment

- Starting Python
- Using the interpreter

- Running a Python script
- Python scripts on Unix/Windows
- Editors and IDEs

Getting Started

- Using variables
- Builtin functions
- Strings
- Numbers
- Converting among types
- Writing to the screen
- Command line parameters

Flow Control

- About flow control
- White space
- Conditional expressions
- Relational and Boolean operators
- While loops
- Alternate loop exits

Sequences

- About sequences
- Lists and list methods
- Tuples
- Indexing and slicing
- Iterating through a sequence
- Sequence functions, keywords, and operators
- List comprehensions
- Generator Expressions
- Nested sequences

Working with files

- File overview
- Opening a text file
- Reading a text file
- Writing to a text file
- Reading and writing raw (binary) data
- Converting binary data with struct

Dictionaries and Sets

- About dictionaries
- Creating dictionaries
- Iterating through a dictionary
- About sets
- Creating sets
- Working with sets

Functions

- Defining functions
- Parameters
- Global and local scope
- Nested functions
- Returning values

Sorting

- The sorted() function
- Alternate keys
- Lambda functions
- Sorting collections

Errors and Exception Handling

- Syntax errors
- Exceptions
- Using try/catch/else/finally
- Handling multiple exceptions
- Ignoring exceptions

Modules and Packages

- The import statement
- Module search path
- Creating modules and Using packages
- Function and Module aliases

Working with Classes

- About o-o programming
- Defining classes
- Constructors
- Methods
- Instance data
- Properties
- Class methods and data

Regular Expressions

- RE syntax overview
- RE Objects
- Searching and matching
- Compilation flags
- Groups and special groups
- Replacing text
- Splitting strings

The standard library

- The sys module
- Launching external programs
- The string module
- Reading CSV data

Dates and times

- Working with dates and times
- Translating timestamps
- Parsing dates from text

Working with the file system

- Paths, directories, and filenames
- Checking for existence
- Permissions and other file attributes
- Walking directory trees
- Creating filters with fileinput
- Security and File Access

Network services

- Grabbing web content
- Detecting Malformed Input

Writing secure Python applications

- Parsing command-line options
- Getting help with pydoc
- Safely handling untrusted data
- Managing eval() permissions
- Potential insecure packages
- Embedding code snippets in Python
- Embedding authentication data in Python
- Potentially dangerous operations:

- File access
- Operating system access
- Calls to external services
- Called to external data sources
- Static analysis tools such as Bandit

Log File Analysis

- Raw log file manipulation
- Fail2Ban
- Customizing Fail2Ban with Python

Security Filters

- SQL-Injection Detection
- ModSecurity CRS filtering

Packet Analysis

- Packet Sniffing in Python

Analytics

- Security Logging and Analytics
- Attack Detection and Defense
- Python and Spark High-Level Overview

Bonus Content / Time Permitting

RESTful Web Services

- What is Flask?

- Developing a Flask Web service
- Mapping resources using URLs
- Mapping resources using HTTP Negotiating data content

Python application security

- OWASP 2021 Top Ten Overview
- Python Code Access Control
- Options for Protecting Data
- Injection and Python
- Python and Data Validation
- Python and XML Processing
- Python and Known Vulnerable Components
- Python and Serialization/Deserialization

Related Courses

TT8120	Web Application Security Essentials: Understanding OWASP Risks and Fixes That Really Work
TT8700	Securing Databases: Practical Database Security Skills for Safer Systems
TTAI2810	Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp
TTPS4800	Introduction to Python Programming Basics
TTPS4820	Mastering Python Programming Boot Camp
TTPS4824	Python Essentials for Networking & Systems Administration

For More Information

Please [contact us](#) or call 844-475-4559 toll free for more information about our training services (instructor-led, self-paced or blended), coaching and mentoring services, public course enrollment or questions, partner programs, courseware licensing options and more.