301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

CYBERPHOENIX

Python Security for Practitioners Training

This 4-day instructor-led training course teaches students how to create their own security defense using the Python programming language.

Course Overview

This training course teaches students how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker's tools, this course will teach students to create their own security defense using the Python programming language. This course demonstrates how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus.

Course Outline

Setting Up Your Python Environment

- nstalling Kali Linux
- WingIDE

The Network: Basics

- Python networking in a paragraph
- TCP Client
- UDP Client
- TCP Server
- Replacing Netcat
- Building a TCP Proxy
- SSH with

- SSH Tunneling

The Network: Raw Sockets and Sniffing

- Building a UDP Host Discovery Tool
- Packet Sniffing on Windows and Linux
- Decoding the IP Layer
- Decoding ICMP

Owning the Network with SCAPY

- Stealing Email Credentials
- ARP Cache Poisoning with SCAPY
- PCAP Processing

Web Hackery

- The Socket Library of the Web: urlib2
- Mapping Open Source Web App Installations
- Bruite-Forcing Directories and File Locations
- Bruite-Forcing HTML form authentication

Extending Burp Proxy

- Setting Up
- Burp Fuzzing
- Bing for Burp
- Turning Website Content into Password Gold

Github Command and Control

- Setting Up a GitHub Account
- Creating Modules
- Trojan Configuration
- Building a GitHub-Aware Trojan

Common Trojaning Tasks on Windows

- Keylogging for Fun and Keystrokes
- Taking Screenshots
- Pythonic Shellcode Execution
- Sandbox Detection

Fun with Internet Explorer

- Main n the Browser
- IE COM Automation for Exfiltration

Windows Privilege Escalation

- Installing the Prerequisites
- Create a Process Monitor
- Windows Taken Privileges
- Winning the Race
- Code Injection

Automating Offensive Forensics

- Installation
- Profiles
- Grabbing Password Hashes
- Direct Code Injection

Python Security for Practitioners Training FAQs

Who should take this course?

This course is intended for security professionals tasked with developing Python applications, Pen testers looking to expand their knowledge into building security tools, and technologists needing customized tool sets.

What is the recommended experience for this course?

Students should have basic experience and understanding of any scripting or programming language.

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Starting at $2,195

ATTENTION

Government Employees & Government Contractors call 240.667.7757 for GSA Pricing.

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

Included in this **Python Security for Practitioners Training**

- 4 days instructor-led training
- Python Security for Practitioners Training training book
- Eligible for MyCAA scholarship
- This course maps to the NICE framework
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*