Hacking with Python

Course Summary

Description

The Gray Hat Hacker Guide to Python

Once you've graduated from our Introduction to Python Scripting course and venture down the path of an Elite Operator, you'll find your way to our latest programming course, Hacking With Python. The Python scripting language has been on an incredible rise as we merge scripting and object oriented programming together in today's rapid development environment. To survive as an Information Assurance analyst today, you must have a good scripting background.

This course teaches you how to use Python to build powerful scripts to push the limits of system security. Designed to be used for Gray Hat Hacking, the course will detail code that can be used to ethically hack into applications and networks to test security. This course is also designed with the Reverse Engineer in mind since automated Malware Analysis is almost essential in this chaotic network warfare world we live in. Python is quickly becoming the adopted language of choice to automate analysis tasks with IDA and OllyDbg. The world's best hackers are using Python to do their handiwork – shouldn't you?

On the fifth day, students will have to apply what they learned all week in a multi-level challenge. In order to progress to the next level of the challenge they have to complete certain tasks. First they'll have to brute force a password from an application and gain entry. Once they gain the password they'll use that password to progress into the next challenge. This continues four times before they can receive the final hacker prize. This is not a trivial challenge and requires the students to fully understand what python code to write, as well as how to implement the code quickly.

Objectives

After taking this course, students will be able to:

- Automate tedious reversing and security tasks
- Design and program your own debugger
- Learn how to fuzz Windows drivers and create powerful fuzzers from scratch
- Have fun with code and library injection, soft and hard hooking techniques, and other software trickery
- Sniff secure traffic out of an encrypted web browser session
- Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more

Topics

- Python as a Hack Tool
- Python as a Reverse Engineering Tool
- Setting up your development environment
- Windows Automation
- Brute Forcing Console Applications
- Using the CTypes Library
- SendKeys Module
- Windows GUI Automation
- Brute Forcing GUI Applications
- Clearing Windows Event Logs
- Multi - Threading in Python
- Building a Python Port Scanner
- Debugger Concepts
- Intel X86 Architecture
- Scripting with PyDBG
- Scripting with Immunity Debugger
- Scripting with IDA Pro
- Process Injection with Python
- Hooking
- Hard Hooking with Immunity Debugger
- Fuzzing
- Py2Exe
- Student Practical Demonstration:

Hacking with Python

Course Summary (cont'd)

Audience

This course is designed for:

- Threat operation analysts seeking a better understanding of malware
- Incident responders who need to quickly address a system security breach
- Forensic investigators who need to identify malicious software
- Individuals who have experimented with malware analysis and want to expand their malware analysis techniques and methodologies

Prerequisites

Before taking this course, students should have a thorough understanding of Microsoft Windows. Attendance of Introduction to Python or equivalent experience with Python 2.7 is required. Knowledge of OllyDbg and IdaPro is recommended.

Duration

Five days