DEV550 – Python for Pentesters

Course Overview

DEV550 – Python for Pentesters is an intermediate level course designed for pentesters who want to use Python to build specialized tools. This challenging course will expose students to target scanning, enumeration, exploit development, web application attacks, and persistence mechanisms through Python scripting.

Upon completion, students will have built an arsenal of over 20 penetration testing tools.

Objectives

- Provide students with the knowledge necessary to analyze technical situations, solving them through the development of Python tools

Target Audience

- This course is designed for students who have basic programming/scripting experience in C or Python, knowledge of networking concepts, and knowledge of penetration testing methods and hacking tools

Estimated Course Length: 24 hours

Day 1

Introduction to building pentesting tools in Python. Students will review Python fundamentals and will develop target scanning and enumeration tools using modules from the Python Standard Library as well as third party modules.

Topics List

- Python Fundamentals
- Socket Module
- I/O Functionality
- User Input
- Application Banner Grabbing
- HTTP Methods
- Nmap Module

Day 2

Students will begin the day by creating custom scanners using the Nmap module. They will develop algorithms to parse complex data sets and build additional functionality into their custom tools.

Topics List

- Building Custom Scanners
- Parsing Nmap Data
- Exception Handling
- Enhancing Tool Functionality
- OS Module
- Introduction to Exploit Development

Day 3

Students will begin the day by taking a deep look at x86 memory architecture, operating system controls and debugging. Students will then learn how to construct exploits against stack-based buffer overflows, as well as how to embed shellcode into their Python scripts.

Topics List

- x86 Memory Architecture
- Exploit Mitigation Controls
- Fuzzing
- Debugging
- Shellcode
- Constructing Exploits

Day 4

Students will learn about common web application vulnerabilities, reconnaissance methods and attack vectors. Students will then write code to identify and exploit Standard Query Language (SQL) and Cross-Site Scripting (XSS) vulnerabilities to reveal server-side details, as well as to find directory traversal vulnerabilities.

Topics List

- Web Application Vulnerabilities
- Web Application Reconnaissance
- HTTP Authentication
- SQL Vulnerabilities
- XSS Vulnerabilities
- Directory Traversal Vulnerabilities

Day 5

On the final day of class, students will learn how to conduct post-exploitation pillaging and employ persistence techniques. They will then learn how to build reverse shells, send encoded data via HTTP requests, and control their persistence tool via command and control mechanisms.

Topics List

- Command and Control Systems
- Persistence
- Subprocess Module
- Encoding and Decoding Data
- Data Exfiltration

About CyberStronger

Comtech provides cybersecurity solutions and services tailored to training and workforce development. The CyberStronger product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech CyberStronger offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.

Comtech
cyberstronger.com | comtechtel.com
275 West Street, Annapolis, MD 21401