KOENIG SOLUTIONS · COURSE OUTLINE

Python Exploits: Sniffers & Malware Reverse Engineering

Learn to use Python to build network sniffers, exploit web and binary vulnerabilities, and reverse engineer malware.

8
MODULES

51
TOPICS

COURSE OVERVIEW

This course begins with core Python fundamentals, including data types, control flow, functions, object-oriented programming and configuring Python across Linux, Windows and mobile platforms. It then covers file, directory and process security, before moving into raw sockets, socket programming and building sniffers and packet injectors. The course continues with web application security, including SQL and XSS attacks, exploit writing with Immunity Debugger, and binary data analysis. It concludes with malware analysis through process debugging and memory patching, attack task automation, and a final consolidation of the concepts covered.

WHO THIS COURSE IS FOR

- **Penetration Testers**
- **Security Analysts**
- **Malware Analysts**
- **Reverse Engineers**
- **Python Developers**
- **Network Security Engineers**

LEARNING OBJECTIVES

- Explain core Python data types, control flow and functions
- Configure Python environments across Linux, Windows and mobile platforms
- Implement file, directory and permission controls in Python
- Apply socket programming to build sniffers and packet injectors
- Analyse web application vulnerabilities such as SQL and XSS attacks
- Develop exploits using Immunity Debugger and Python plugins
- Assess malware behaviour through process debugging and memory patching
- Automate security tasks using Python libraries

COURSE SYLLABUS

8 Modules, 51 Topics

01

Python – Basic Fundamental

TOPICS

- Introduction to Python
- Data Types and variables
- Statement Documentations and help
- String Revisited
- Control Flow and Data structure
- Functions, Functional Programming and File Handling
- Accessing the network and Internet
- Exception Handling
- Modular Programming
- Object Oriented Programming
- Modules, Packages and Distribution
- Configure Python in Linux and Unixes
- Configure Python in Windows
- **How to use Python in Mobiles:** iPhone and Androids
- Python Program Portability
- Python Framework and IDEs

02

Managing Files, Directory and Security

TOPICS

- Input/output file system in Python
- Creating Managing File and Directory Access
- Use of Multithreading and Concurrency
- How, what and why Inter Process Communication (IPC)
- How to set Permissions and Controls

03

Creating Sniffers and Packet Injector

TOPICS

An Introduction to Raw Socket basics · Python Database access · Porting Python code · Socket Programming with Python · Servers and Clients architecture · Creating Sniffers (wired and wireless) · Creating packet injector

04

Web Application Security

TOPICS

- Introduction to web server and Application server
- Client Side scripting
- Intro to web application and penetration testing in web application
- HTML and XML file analysis
- Web Browser Equality
- Attacking Web Services and Countermeasure
- How and why to use Application Proxies and Data Mangling
- SQL and XSS attacks on web Application
- Intro to Buffer overflow and CSRF

05

Exploitation Writing and Analysis Automation

TOPICS

Exploit Writing Implementation · Immunity Debuggers and Libs · Creating plugins in Python · Binary data analysis · Exploit analysis Automation

06

Malware Analysis and Reverse Engineering

TOPICS

Basics of Process Debugging · Pydbg and its applications · Analyzing live applications · Setting breakpoints, reading memory etc. · In-memory modifications and patching

07

Setting Attack Task Automation

TOPICS

Task Automation with Python · Libraries and Applications

08

Conclusion and Checklist

TOPICS

Course consolidation · Interesting project ideas to pursue

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training | Live Online Classes (ILO) | Fly-Me-A-Trainer (FMAT) | Flexi (Self-Paced) | 1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com | info@koenig-solutions.com