



PYTHON TRAINING

Security With Python

Master Python for ethical hacking, penetration testing, and digital forensics to secure systems.

DURATION

2 hours

LEVEL

Intermediate

FORMAT

Instructor-Led

- Globally Recognized Certification

- Expert-Led Hands-On Training

- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

This intermediate-level "Security With Python" course is meticulously designed to equip aspiring cybersecurity professionals and developers with the essential skills to leverage Python for robust security tasks. Python's versatility makes it an indispensable tool for automating security processes, performing vulnerability assessments, and developing custom security solutions. Over two intensive hours, you will delve into practical applications of Python in the cybersecurity landscape, understanding how to build scripts for network scanning, web vulnerability analysis, and data protection, thereby enhancing your ability to defend against modern cyber threats. We will cover fundamental libraries and techniques crucial for security operations, moving beyond theoretical concepts to hands-on implementation.

By completing this course, participants will gain a deep understanding of how Python can be utilized for ethical hacking, penetration testing, and incident response automation. You will learn to write scripts that can identify network weaknesses, interact with web applications to discover common vulnerabilities, and implement basic cryptographic principles. The professional benefits are immense, enabling you to automate repetitive security tasks, streamline your workflow, and contribute more effectively to securing digital assets. This training is ideal for individuals looking to bridge their Python programming skills with the high-demand field of cybersecurity, preparing them for specialized roles in threat analysis and security development.

Duration	2 hours
Level	Intermediate
Vendor	Python

COURSE CURRICULUM

01 Module 1: Python Fundamentals for Security

- Setting up your security Python environment
- Essential Python libraries for network interactions (socket, requests)
- File system access and manipulation for forensics
- Basic command-line argument parsing for security tools

02 Module 2: Network Reconnaissance and Scanning with Python

- Developing custom port scanners
- Banner grabbing techniques
- Host discovery (ping sweeps) with Python
- Introduction to Scapy for packet crafting and sniffing

03 Module 3: Web Vulnerability Analysis with Python

- Automating web requests and responses using 'requests' library
- Scripting for common web vulnerabilities (e.g., XSS, SQLi detection basics)
- Brute-forcing login pages
- Web scraping for intelligence gathering

04 Module 4: Data Security and Cryptography Basics in Python

- Implementing hashing algorithms (MD5, SHA-256)
- Symmetric and asymmetric encryption principles with Python (basic examples)
- Secure password storage techniques
- File encryption and decryption utilities

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

- > **Security Automation Engineer**
- > **Junior Penetration Tester**
- > **Cybersecurity Scripting Specialist**

FREQUENTLY ASKED QUESTIONS

Q: What level of prior Python programming experience is required to effectively benefit from this 'Security With Python' course?

This course is designed for individuals with intermediate Python programming skills. You should be comfortable with Python's basic syntax, data structures (lists, dictionaries), functions, and object-oriented programming (classes and objects). While no prior cybersecurity experience is strictly required, a basic understanding of networking concepts will be beneficial for modules on network reconnaissance.

Q: How will the skills learned in this course enhance my ability to identify and mitigate cyber threats in a professional environment?

This course will equip you with practical Python scripting abilities to proactively identify and mitigate threats. You will learn to develop custom tools for scanning networks, detecting web vulnerabilities, and automating security checks, which are crucial for penetration testing and vulnerability assessments. These skills directly translate into a greater capacity to understand attack vectors, build defensive scripts, and contribute to a more secure operational environment.

Q: What specific types of custom security tools or automated scripts will I be equipped to develop after completing this 'Security With Python' course?

Upon completion, you will be able to develop a range of custom security tools. This includes creating your own port scanners, network host discovery scripts, basic web vulnerability scanners (for XSS, SQLi detection), and brute-forcing utilities. Furthermore, you'll gain the foundational knowledge to implement scripts for file encryption/decryption, secure password management, and automating routine security tasks, significantly boosting your productivity and effectiveness in cybersecurity roles.

ABOUT COMPUTER PRIDE



East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+

10,000+

50+

Years of Excellence

Professionals Trained

Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location

1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email

info@computer-pride.co.ke

Phone

+254 705 900 900

www.computer-pride.co.ke