



PYTHON TRAINING

Python For Cybersecurity

Master Python scripting for cybersecurity. Learn to automate threat detection, analysis, and ethical hacking techniques.

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 course, "Python For Cybersecurity," is meticulously designed to equip IT professionals and aspiring cybersecurity experts with the essential skills to leverage Python for robust security operations. You'll delve into the practical application of Python scripting for automating security tasks, performing network analysis, detecting vulnerabilities, and responding to incidents. The curriculum emphasizes hands-on exercises, demonstrating how Python acts as a versatile tool for enhancing an organization's defensive and offensive security capabilities. You will learn to integrate Python with various security tools and protocols, providing you with a powerful skill set in a rapidly evolving threat landscape.

By mastering Python in a cybersecurity context, you will gain a significant advantage in areas such as penetration testing, digital forensics, security automation, and threat intelligence. The course covers key Python libraries like Scapy for packet manipulation, Nmap for network scanning, Requests for web interactions, and libraries for parsing log files and interacting with APIs. This expertise translates directly into improved efficiency, the ability to build custom security tools, and a deeper understanding of network and system vulnerabilities, ultimately enhancing your value in any security team.

Duration	2 hours
Level	Intermediate
Vendor	Python

COURSE CURRICULUM

01 Module 1: Python Fundamentals for Security

- Setting up a Python security environment
- Review of essential Python data structures and control flow
- File I/O and command-line arguments
- Introduction to Socket programming for network communication
- Working with common security-focused Python libraries

02 Module 2: Network Scanning and Reconnaissance with Python

- Building custom port scanners
- Automating Nmap scans with Python-Nmap
- Packet sniffing and analysis using Scapy
- DNS enumeration and sub-domain discovery
- Geo-location and IP intelligence gathering

03 Module 3: Vulnerability Analysis and Exploitation Scripting

- Developing Python scripts for banner grabbing
- Fuzzing applications for vulnerabilities
- Crafting exploit prototypes for common vulnerabilities (e.g., buffer overflows, SQL injection)
- Interacting with web applications using Requests and Beautiful Soup
- Automating brute-force and dictionary attacks

04 Module 4: Digital Forensics and Incident Response with Python

- Parsing log files for suspicious activities
- Automating forensic data collection from endpoints
- Analyzing network traffic captures (PCAPs) using Scapy
- Memory forensics basics with Python

- Developing scripts for rapid incident containment and analysis

05 Module 5: Web Application Security and Automation

- Automating web vulnerability scanning
- Exploiting common web vulnerabilities (XSS, CSRF) with Python
- Session management and cookie manipulation
- Interacting with RESTful APIs for security automation
- Building custom web crawlers for security audits

06 Module 6: Security Tool Integration and Reporting

- Integrating Python with SIEM/SOAR platforms
- Automating security reports and data visualization
- Building custom security dashboards
- Introduction to cryptographic operations in Python
- Best practices for secure Python coding

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

- > **Junior Penetration Tester specializing in custom script development**
- > **Security Automation Engineer utilizing Python for SIEM/SOAR integration**
- > **Incident Response Analyst focused on forensic data collection and analysis**

FREQUENTLY ASKED QUESTIONS

Q: What specific Python libraries and frameworks will I gain hands-on experience with in this course for cybersecurity applications?

This course provides extensive hands-on experience with key Python libraries essential for cybersecurity. You will master libraries such as Scapy for crafting and analyzing network packets, Python-Nmap for automating network discovery and port scanning, the Requests library for interacting with web applications and APIs, and BeautifulSoup for parsing HTML content. Additionally, you'll work with standard libraries for file I/O, socket programming, and regular expressions, all crucial for building robust security tools and scripts.

Q: How does this 'Python For Cybersecurity' course directly contribute to my ability to perform real-world penetration testing or incident response tasks?

This course directly enhances your capabilities in penetration testing and incident response by teaching you to build custom tools for various phases. For pen testing, you'll learn to script reconnaissance, automate vulnerability scanning, and craft exploit prototypes, moving beyond off-the-shelf tools. For incident response, you'll gain skills in automating log analysis, forensic data collection, and network traffic examination, enabling faster detection, analysis, and containment of security breaches with tailored Python scripts.

Q: Is prior cybersecurity knowledge a prerequisite for this intermediate-level Python For Cybersecurity course, or is solid Python programming experience sufficient?

While prior exposure to basic networking concepts and operating system fundamentals is beneficial, solid intermediate-level Python programming experience is the primary prerequisite for this course. You should be comfortable with Python

syntax, data structures, functions, and object-oriented programming basics. We will introduce cybersecurity concepts as they relate to Python scripting, but a foundational understanding of how networks and systems operate will help you grasp the security applications more quickly.

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+

Years of Excellence

10,000+

Professionals Trained

50+

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