



PYTHON TRAINING

Python For Security Professionals

Master Python for cybersecurity. Learn to automate tasks, analyze threats, and build robust security tools.

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 Security Professionals," is meticulously designed for cybersecurity practitioners, IT administrators, and aspiring security experts who aim to harness the power of Python for advanced security tasks. In today's rapidly evolving threat landscape, the ability to automate, analyze, and respond quickly is paramount. Python, with its simplicity and extensive library ecosystem, has become an indispensable tool for security professionals seeking efficiency and deeper insights into security operations.

Throughout this 2-hour intensive program, participants will delve into practical applications of Python, learning to develop custom scripts for a wide array of security functions. Core technologies covered include Python's standard library for system interaction, specialized modules for network programming (sockets, Scapy), web interaction (requests, BeautifulSoup), cryptography, and file system forensics. The course emphasizes hands-on scripting to solve real-world security challenges, ranging from automating vulnerability assessments and network reconnaissance to building forensic tools and enhancing incident response capabilities.

Upon completion, attendees will possess a robust skill set for automating repetitive security tasks, developing custom security tools, performing data analysis for threat intelligence, and significantly improving their overall effectiveness in defending digital assets. This course will empower you to move beyond off-the-shelf solutions and craft tailor-made scripts that precisely meet your organization's unique security requirements, ultimately boosting your career trajectory in specialized cybersecurity roles.

Duration	2 hours
Level	Intermediate
Vendor	Python

COURSE CURRICULUM

01 Module 1: Python Fundamentals for Security Scripting

- Review of Python essentials: data types, control flow, functions
- Setting up a secure Python development environment
- Introduction to relevant Python modules: ``os``, ``sys``, ``subprocess``
- Handling files and directories securely

02 Module 2: Network Reconnaissance & Scanning with Python

- Basic socket programming for network communication
- Developing custom TCP and UDP port scanners
- Leveraging Scapy for packet crafting and network analysis
- Automating Nmap scans and parsing output with Python

03 Module 3: Web Security Scripting and API Interaction

- Using the ``requests`` library for HTTP interactions
- Scripting for web vulnerability detection (e.g., basic XSS/SQLi checks)
- Interacting with RESTful security APIs (e.g., VirusTotal, SIEMs)
- Introduction to web scraping for Open-Source Intelligence (OSINT)

04 Module 4: Cryptography, Forensics, and Log Analysis

- Implementing hashing and encryption with Python's ``hashlib`` and ``cryptography`` libraries

- Scripting for file system forensics: metadata extraction, file carving basics
- Automating log file parsing and analysis (e.g., syslog, web server logs)
- Basic malware analysis scripting: string extraction, indicator generation

05 Module 5: Security Automation and Incident Response

- Developing scripts for automated vulnerability assessment workflows
- Building tools for incident response: host data collection, alert enrichment
- Automating security tasks across platforms using SSH and WinRM with Python
- Creating custom reporting and visualization for security events

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

- > **Security Automation Engineer**
- > **Penetration Tester / Ethical Hacker (Scripting Specialist)**
- > **Security Operations Center (SOC) Analyst (Advanced Scripting Focus)**

FREQUENTLY ASKED QUESTIONS

Q: What specific security tools or frameworks will I learn to automate or interact with using Python in this course?

This course focuses on teaching you the foundational Python scripting skills to interact with and automate various security tools and protocols. You will learn to automate Nmap scans and parse their results, craft network packets using Scapy, make API calls to threat intelligence platforms like VirusTotal, and interact with web applications for vulnerability checks. While we won't deep-dive into the internal workings of every commercial security product, you'll gain the universal Python knowledge to script integrations with SIEMs, firewalls, and other security solutions via their APIs.

Q: Is prior cybersecurity experience required, or is this course suitable for IT professionals new to security who want to leverage Python?

While foundational IT knowledge is beneficial, this course is primarily tailored for individuals who already have a basic understanding of cybersecurity concepts and networking fundamentals. It is ideal for security analysts, network engineers, or system administrators looking to enhance their existing security skill set by incorporating Python for automation and tool development. While we cover Python fundamentals relevant to security, it's an intermediate-level course that assumes some familiarity with security operations rather than introducing security from scratch.

Q: How will completing this course enhance my ability to perform incident response or threat hunting tasks?

Upon completing this course, you will significantly enhance your capabilities in incident response and threat hunting by being able to develop custom Python scripts. You'll learn to automate the collection of critical forensic data from endpoints and networks, parse and analyze vast amounts of log data for indicators of compromise, and interact with threat intelligence APIs to enrich security alerts. This empowers you to create more efficient detection mechanisms, accelerate investigation processes, and build bespoke tools that precisely target the unique threats faced by your organization, moving beyond manual processes and generic solutions.

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