



PYTHON TRAINING

Python For Penetration Tester Training Certification Course

Master Python for ethical hacking. Learn to build custom tools and automate penetration testing tasks effectively.

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

Unlock the power of Python to elevate your penetration testing capabilities with Computer Pride's specialized 'Python For Penetration Tester Training Certification Course'. This intensive 2-hour program is meticulously designed for intermediate-level security professionals seeking to automate and enhance their ethical hacking toolkit. You will dive into leveraging Python's versatility to perform critical security tasks, moving beyond manual processes to implement efficient, custom solutions for reconnaissance, vulnerability assessment, and exploitation. This course focuses on practical scripting to build custom tools and integrate with existing security frameworks.

By the end of this certification, you will possess a strong command of applying Python scripting to real-world penetration testing scenarios, significantly boosting your efficiency and effectiveness in identifying and mitigating security vulnerabilities. You will gain hands-on experience with powerful Python libraries tailored for network analysis, web exploitation, and creating bespoke security utilities. This expertise not only streamlines your current workflows but also positions you as a highly adaptable security professional capable of developing innovative solutions in an ever-evolving threat landscape. This foundational training serves as a launchpad for more advanced security automation and custom tool development, directly impacting your ability to deliver comprehensive security assessments.

Duration	2 hours
Level	Intermediate
Vendor	Python

COURSE CURRICULUM

01 Module 1: Python Essentials for Offensive Security

- Quick review of Python fundamentals relevant to scripting
- Setting up a Python security environment (virtual environments, common libraries)
- Basic I/O, file handling, and command-line argument parsing
- Introduction to common networking concepts (sockets, HTTP requests)

02 Module 2: Network Reconnaissance and Scanning with Python

- Building a basic port scanner with `socket`
- Host discovery with `scapy` (introduction)
- Automating DNS enumeration with `dnspython`
- Leveraging `requests` for web server reconnaissance

03 Module 3: Basic Vulnerability Exploitation with Python

- Crafting simple network service exploits (e.g., banner grabbing, simple protocol interaction)
- Introduction to brute-forcing login pages with `requests`
- File upload vulnerabilities (basic exploitation concepts)
- Introduction to creating shellcode runners (basic concept)

04 Module 4: Automating Security Tasks & Reporting

- Creating scripts for data parsing and log analysis
- Automating report generation (e.g., exporting findings to CSV/JSON)
- Introduction to integrating Python with external tools (e.g., running Nmap via Python)
- Best practices for secure Python scripting

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

- > **Penetration Testing Scripting Specialist**
- > **Junior Security Automation Engineer**
- > **Ethical Hacking Tool Developer**

FREQUENTLY ASKED QUESTIONS

Q: What foundational knowledge should I have before enrolling in this 'Python For Penetration Tester' course?

This course is designed for individuals at an intermediate level. You should have a solid understanding of fundamental Python programming concepts (variables, data types, loops, functions, basic object-oriented programming) and a basic grasp of networking principles (IP addresses, ports, common protocols like TCP/IP, HTTP). Prior exposure to security concepts is beneficial but not strictly required for the Python scripting aspects.

Q: How will this specific course enhance my ability to conduct penetration tests, beyond just learning Python syntax?

This course goes beyond mere syntax by focusing on the practical application of Python for penetration testing. You will learn to build custom tools for network scanning, automate reconnaissance tasks, craft simple exploits, and parse security-related data. The emphasis is on developing a mindset to solve pen-testing challenges efficiently with code, enabling you to create bespoke solutions where off-the-shelf tools might fall short, thus significantly speeding up and customizing your assessment methodologies.

Q: Will this certification prepare me to develop complex security tools or contribute to open-source pen-testing projects?

While this 2-hour certification provides a strong foundational understanding and hands-on experience in using Python for immediate penetration testing tasks, it serves as a crucial stepping stone. It will equip you with the essential scripting skills and methodologies necessary to begin developing your own advanced security tools and contribute to open-source projects. For more complex tool development or deep contributions, further specialized learning and extensive practical experience would be recommended, building directly on the skills acquired here.

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