



# CA202: Python Programming Language

16 Instructional Hours

24 CPEs

8 Labs



LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON



BEGINNER

This course provides a comprehensive introduction to Python programming, covering both foundational concepts and practical applications. It begins with core syntax, data types, and control structures, then progresses into functions, modules, file handling, and data structures. The course also explores object-oriented programming, exception handling, and advanced topics such as threading and networking. Throughout the learning journey, hands-on “Cyberdrome” exercises reinforce concepts with real-world cybersecurity use cases, enabling learners to apply Python in automation, data processing, and security-related tasks.

## You Will Be Able To



- Write and execute Python scripts using proper syntax, variables, and data types
- Implement control flow, loops, and functions to build structured programs
- Manipulate files, directories, and structured data formats such as CSV and JSON
- Apply object-oriented programming principles including classes, inheritance, and polymorphism
- Handle exceptions and debug programs effectively for reliable execution
- Develop basic cybersecurity-related scripts such as IP filtering, password validation, and port scanning

## Who Should Attend



This course is designed for beginners and early-stage learners who want to build a solid foundation in Python programming. It is suitable for students, aspiring developers, and cybersecurity enthusiasts who have little to no prior programming experience. The course is also appropriate for individuals seeking to transition into technical roles where scripting, automation, and data handling are essential skills.

## Relevant Combat Roles



- Cybersecurity Analyst
- SOC Analyst (Tier 1 / Tier 2)
- Automation / Scripting Engineer
- Penetration Tester

## Topics Covered



### Network & Sockets Labs

Build TCP client/server apps and monitor connections to detect unusual port activity.

### Data Protection & File Security

Implement DLP checks, file integrity monitoring, and audit access to sensitive files.

### Security Automation with Python

Develop scripts for IP blocking, password auditing, phishing detection, and rule-based alerts.

### Library Hijacking & Serialization Labs

Explore Python import behavior, unsafe dependency handling, and serialization/deserialization risks in controlled lab scenarios.

### Malware Analysis & OCR Libraries

Use Python for safe malware analysis concepts in sandboxed environments and work with OCR libraries to extract and process text from images.

### Data Handling & Ethical Web Use

Process CSV/JSON logs and perform compliant web scraping on approved sources.

## Labs



### Python Automation & Web Scraping Development

(web scraping, data collection, and structured data storage using Python)

### Computer Vision & OpenCV Projects

(face detection systems, image processing, and OpenCV-based automation)

### Security Monitoring & Exfiltration Detection

(network traffic analysis, anomaly detection, and suspicious transfer monitoring)

### Safe Malware Simulation & Code Mutation Demonstrations

(polymorphic code structure demonstrations in isolated lab environments)

### Remote Administration & Secure Lab Tooling

(controlled remote command execution tools for authorized testing environments)