Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Python 3 for InfoSec Professionals

Course Description & Overview

SecureNinja's Python 3 for InfoSec Professionals course is designed to provide cybersecurity practitioners with the essential programming skills required to automate security tasks, analyze threats, and develop custom security tools. Python is a powerful and widely used language in the cybersecurity industry, making it an invaluable skill for security analysts, penetration testers, forensic investigators, and security researchers.

This course introduces participants to Python programming fundamentals while demonstrating real-world applications in cybersecurity, including log analysis, network security, malware analysis, digital forensics, web application security, and exploit development. With hands-on exercises, students will learn how to write Python scripts to automate security tasks, parse logs, analyze network traffic, interact with APIs, develop security testing tools, and detect security vulnerabilities.

By the end of this course, participants will have the ability to:

•Write custom Python scripts for security automation and analysis.

• Parse and analyze log files, PCAP files, and security event data.

•Develop network security tools, such as port scanners and custom backdoors.

•Automate password cracking techniques and perform brute-force attacks.

•Conduct malware analysis and reverse engineering with Python-based tools.

•Write Burp Suite extensions for web application security testing.

• Perform security assessments and vulnerability exploitation using Python.

The hands-on nature of this course ensures that participants not only learn Python programming but also apply it in real-world security scenarios. Whether you are a security analyst looking to automate threat detection, a penetration tester developing custom exploits, or a forensic investigator analyzing digital evidence, this course will equip you with the Python skills necessary to enhance your cybersecurity expertise.

Why Choose This Course?

•Security-Focused Python Training: Learn Python with a focus on its applications in cybersecurity.

•Hands-On Labs: Apply concepts immediately with interactive exercises and real-world security scenarios.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

•Covers Key InfoSec Domains: Learn Python for network security, malware analysis, penetration testing, forensics, and more.

•Essential Skill for Cybersecurity Professionals: Python is widely used in security automation, making it a must-have skill for InfoSec experts.

•Applicable to Various Security Roles: Whether you are a penetration tester, SOC analyst, or forensic investigator, Python will enhance your capabilities.

Topics Covered

•Python fundamentals and scripting essentials

•Log analysis and file parsing

•Regular expressions for data extraction

•Functions and classes for efficient scripting

•Digital forensics applications with Python

•Parsing PCAP files for network traffic analysis

•Malware analysis and reverse engineering with Python

•Network security testing, including socket programming

•Password cracking techniques using Python

•Web application security testing with Python scripts

•Writing Burp Suite extensions for web security testing

•Exploit development and vulnerability research

Who is it for?

•Security professionals looking to automate tasks and enhance their efficiency

•Penetration testers and red team members who need custom tools for assessments

•Security analysts and SOC teams looking to improve threat detection and analysis

•Digital forensics professionals working with evidence extraction and log analysis

•Ethical hackers and bug bounty hunters looking to expand their skillset

•IT administrators who want to implement security automation

Who Would Benefit?

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

•Cybersecurity professionals seeking to learn Python for security applications

•IT professionals transitioning into security roles

•SOC analysts looking for automation techniques to improve threat detection

•Ethical hackers and penetration testers needing custom tools

•Digital forensics specialists working on investigations

Prerequisites

While ther are no mandatory prerequisits for this course, we do recommend:

•Basic understanding of cybersecurity concepts

•Familiarity with command-line interfaces (Linux and Windows)

•Some programming experience is beneficial but not required

Course Outline

Module 1: Python Fundamentals

•Installing Python

•Basic syntax, printing, and math operations

•Variables, functions, and modules

•Working with strings, lists, and sequences

Module 2: Parsing Files with Python

•Introduction to log analysis

•Reading files line by line with Python

•Parsing and formatting CSV files

Module 3: Regular Expressions

•Using regex for data extraction

•Pattern matching and text manipulation

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Module 4: Functions & Classes

•Writing reusable functions

•Understanding Python classes and object-oriented programming

Module 5: Digital Forensics with Python

•Extracting and analyzing digital evidence

•Making forensic reports searchable using OCR and ElasticSearch

Module 6: Parsing PCAP Files

•Analyzing network traffic captures using Python

•Identifying malicious traffic patterns

Module 7: Malware Analysis

•Introduction to malware reverse engineering

•Automating malware analysis with Python

•Creating and maintaining a malware database

Module 8: Network Testing with Python

•Socket programming for network communication

•Developing TCP and UDP clients and servers

•Writing custom bind and reverse shells

Module 9: Password Cracking with Python

•Cracking password hashes using Python

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

•Automating brute-force attacks on authentication systems

Module 10: Web Application Security Testing

•Automating security testing with Python

•Checking HTTP headers and identifying security misconfigurations

•Performing SQL injection, XSS, and file inclusion attacks

Module 11: Writing Burp Suite Extensions

•Developing custom extensions for web application security testing

•Automating attack scenarios with Burp API

Module 12: Exploit Development

•Understanding stack overflows and SEH overwrites

•Writing custom exploits using Python

Course Length

- 5 Days
- 40 Hours

By the end of the course, participants will have a strong understanding of Python for security applications and the ability to develop custom security tools and scripts for automation, analysis, and penetration testing.