uCertify

Course Outline

Learn Penetration Testing with Python

30 Oct 2025

1. Exercises, Quizzes, Flashcards & Glossary

   Number of Questions
2. Expert Instructor-Led Training
3. ADA Compliant & JAWS Compatible Platform
4. State of the Art Educator Tools
5. Award Winning Learning Platform (LMS)
6. Chapter & Lessons

   Syllabus

   Chapter 1: Preface

   Chapter 2: Starting with Penetration Testing and Basic Python

   Chapter 3: Cracking with Python 3

   Chapter 4: Service and Applications Brute Forcing with Python

   Chapter 5: Python Services Identifications: Ports and Banner

   Chapter 6: Python Network Modules and Nmap

   Chapter 7: Network Monitoring with Python

   Chapter 8: Attacking Wireless with Python

   Chapter 9: Analyze Web Applications with Python

   Chapter 10: Attacking Web Applications with Python

   Chapter 11: Exploit Development with Python

   Chapter 12: Forensics with Python

   Chapter 13: Python with Burp Suite

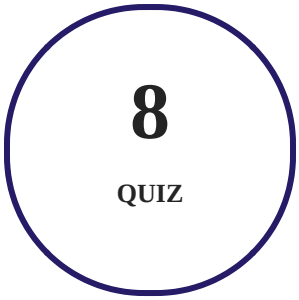
   Chapter 14: Fuzzing with Python

   Chapter 15: ChatGPT with Python

   Videos and How To

1. Quiz

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.



2. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

3. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

4. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

5.  Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
    1. Best Postsecondary Learning Solution

- **2015**
    1. Best Education Solution
    2. Best Virtual Learning Solution
    3. Best Student Assessment Solution
    4. Best Postsecondary Learning Solution
    5. Best Career and Workforce Readiness Solution
    6. Best Instructional Solution in Other Curriculum Areas
    7. Best Corporate Learning/Workforce Development Solution

- **2016**
    1. Best Virtual Learning Solution
    2. Best Education Cloud-based Solution
    3. Best College and Career Readiness Solution
    4. Best Corporate / Workforce Learning Solution
    5. Best Postsecondary Learning Content Solution
    6. Best Postsecondary LMS or Learning Platform
    7. Best Learning Relationship Management Solution

- **2017**
    1. Best Overall Education Solution
    2. Best Student Assessment Solution
    3. Best Corporate/Workforce Learning Solution
    4. Best Higher Education LMS or Learning Platform

- **2018**
    1. Best Higher Education LMS or Learning Platform
    2. Best Instructional Solution in Other Curriculum Areas
    3. Best Learning Relationship Management Solution

- **2019**
    1. Best Virtual Learning Solution
    2. Best Content Authoring Development or Curation Solution
    3. Best Higher Education Learning Management Solution (LMS)

- **2020**
    1. Best College and Career Readiness Solution
    2. Best Cross-Curricular Solution
    3. Best Virtual Learning Solution

6.  Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: Preface

Chapter 2: Starting with Penetration Testing and Basic Python

- Introduction
- Introducing penetration testing
- Penetration testing types
- Penetration testing tools
- The basics of Python 3
- Python variables
- Statements in Python 3
- Operators in Python 3
- Functions in Python 3
- Classes, self, and destructors in Python 3
- Conclusion
- Programming questions

Chapter 3: Cracking with Python 3

- Introduction
- Types of crypto world

- Types of credential attacks
- Attacking passwords with Python
- Conclusion

Chapter 4: Service and Applications Brute Forcing with Python

- Introduction
- Services brute forcing
- SMTP brute forcing
- FTP brute force attack
- SSH brute force attack
- Web broken authentication
- Conclusion

Chapter 5: Python Services Identifications: Ports and Banner

- Introduction
- Deeper inside systems communication
- Ethernet networks
- Ethernet frames architecture
- Wireless networks

- IP packet architecture
- TCP packet header
- UDP packet header
- TCP three-way handshake
- Wireless four-way handshake
- Services uncovered by Python
- Socket library
- Python port scanner
- Python live host check
- Python DNS
- Conclusion

Chapter 6: Python Network Modules and Nmap

- Introduction
- Python Nmap
- Python network modules
- Understanding Scapy
- Network discovery with Scapy
- Fuzz method

- TCP SYN-ACK ping methods
- ARP ping method
- Scapy UDP ping
- Scapy traceroute
- Scapy port scanner
- Create custom packet
- ICMP packet header
- Conclusion

Chapter 7: Network Monitoring with Python

- Introduction
- Understanding network monitoring
- Network monitoring and its importance
- Understanding network tools
- Security Operation Center
- Network monitoring using socket library
- Monitoring and analysis with SCAPY
- Scapy HTTP monitoring

- Scapy DNS monitoring
- Conclusion

Chapter 8: Attacking Wireless with Python

- Introduction
- 802.11 packet headers
- Wireless frequency and channels
- Wireless BSSID and SSID and ESSID
- Wireless encryption family
- Wireless SSID using Scapy
- Deauthentication using Python
- Conclusion

Chapter 9: Analyze Web Applications with Python

- Introduction
- HTTP methods with Python
- Python modules
- Parsing URLs
- Extracting cookies

- Extracting images and documents
- Images metadata
- Hidden web directories
- Conclusion

Chapter 10: Attacking Web Applications with Python

- Introduction
- Information gathering with Shodan
- Cross-site trace
- Identifying web application firewalls
- Cross-site scripting
- Open redirect with Python
- Bypassing web application firewalls
- Encoding your payload
- Business logic vulnerabilities
- Conclusion

Chapter 11: Exploit Development with Python

- Introduction

- Intel CPU architecture (x86)
- General purpose registers
- Special purpose registers
- Segment registers
- EFLAGS register
- X64 registers
- Windows memory structure
- Big and little endian
- Playing with the stack
- Debugger tools
- Immunity Debugger
- Fuzzing
- Basic buffer overflow
- Removing bad characters
- Building our exploit
- Exploit development protections
- Conclusion

Chapter 12: Forensics with Python

- Introduction
- File analysis
- File metadata
- Analyzing PDF files
- Analyzing TXT files
- Data visualization
- Network forensics
- Conclusion

Chapter 13: Python with Burp Suite

- Introduction
- Burp Suite features
- Burp Suite extensions
- Jython
- Detecting misconfiguration
- Cross-origin resource sharing
- Sensitive data exposure
- Default credentials or pages

- Detecting vulnerabilities
- Detecting cross-site scripting
- Burp Suite Professional
- OWASP Zed Attack Proxy
- Conclusion

Chapter 14: Fuzzing with Python

- Introduction
- Importance of fuzzing in security testing
- Fundamentals of Python in fuzzing
- Types of fuzzing techniques
- Designing a basic fuzzer in Python
- Advanced fuzzing concepts with Python
- Fuzzing network protocols with Python
- Creating fuzzers for executables
- Famous tools used in fuzzing executables
- Fuzzing Windows executables
- Fuzzing Linux executables
- Creating fuzzers for web applications

- Challenges and limitations of fuzzing with Python
- Conclusion

Chapter 15: ChatGPT with Python

- Introduction
- Generating and completing code
- Enhancing code quality and efficiency
- Leveraging ChatGPT in Machine Learning projects
- Integrating ChatGPT with Python libraries and frameworks
- Challenges and best practices in ChatGPT-Python integration
- Conclusion