Password Technical College
44 Calle Félix Arce Lugo
San Germán, PR 00683
https://passwordtech.org

SYLLABUS

GENERAL INFORMATION

Course Title:	CompTIA PenTest+
Code:	PT0-002
Contact Hours:	40
Academic Term:	TBA

COURSE DESCRIPTION

The CompTIA PenTest+ course is an advanced program tailored to train individuals in the practices of systematic penetration testing and vulnerability assessment. This course equips participants with the skills necessary to conduct hands-on penetration testing to identify, exploit, report, and manage vulnerabilities on a network. Upon completion, students will be able to perform penetration tests using a comprehensive and repeatable process and prepare for the CompTIA PenTest+ certification exam, globally recognized as a standard of excellence in the field of penetration testing. This course is ideal for cybersecurity professionals, system and network analysts, and anyone interested in enhancing their knowledge of security through offensive measures.

GENERAL OBJECTIVES

Throughout the course, students will engage in both theoretical learning and practical exercises that cover a broad range of topics related to ethical hacking and penetration testing. The curriculum includes:

- Ethical Hacking Fundamentals: Understand ethical hacking principles, the penetration testing process, and legal compliance.
- Planning and Scoping Penetration Tests: Learn to plan, scope, and manage vulnerabilities assessments and penetration tests.
- Information Gathering and Vulnerability Identification: Techniques for effectively gathering data and identifying system vulnerabilities.
- Attacks and Exploits: Execute network, application, and system exploitation techniques to evaluate security weaknesses.
- Reporting and Communication: Develop comprehensive reports and communicate findings to enhance the security posture of the organization.

- Tools and Scripting: Utilize various tools and scripting languages to automate tasks and improve testing efficiency.

COURSE CONTENT

Lesson 1: Scoping Organizational/Customer Requirements

Lesson 2: Defining the Rules of Engagement

Lesson 3: Footprinting and Gathering Intelligence

Lesson 4: Evaluating Human and Physical Vulnerabilities

Lesson 5: Preparing the Vulnerability Scan

Lesson 6: Scanning Logical Vulnerabilities

Lesson 7: Analyzing Scanning Results

Lesson 8: Avoiding Detection and Covering Tracks

Lesson 9: Exploiting the LAN and Cloud

Lesson 10: Testing Wireless Networks

Lesson 11: Targeting Mobile Devices

Lesson 12: Attacking Specialized Systems

Lesson 13: Web Application-Based Attacks

Lesson 14: Performing System Hacking

Lesson 15: Scripting and Software Development

Lesson 16: Leveraging the Attack: Pivot and Penetrate

Lesson 17: Communicating During the PenTesting Process

Lesson 18: Summarizing Report Components

Lesson 19: Recommending Remediation

Lesson 20: Performing Post-Report Delivery Activities

Password Technical College
44 Calle Félix Arce Lugo
San Germán, PR 00683
https://passwordtech.org

EVALUATION CRITERIA

Criteria	Grade Total
Mid-Term Exam	100
Final Exam	100
Quizzes	100
Assessment	100
Laboratories	100
Total	**500**

Assignments are due in class on the designated day. Late submissions will incur a penalty of one letter grade per day late, unless previously discussed and approved for extension.

EDUCATIONAL RESOURCES

Bock, L., Flefel, H., (2021). The Official CompTIA PenTest+ Guide (PT0-002). CompTIA Inc., Downers Grove, Illinois.
ISBN: 978-1-64274-374-6

NOTES

Reasonable Accommodation: Any student needing accommodation should make a request at the beginning of the course or as soon as possible thereafter.

Academic Integrity: Honesty, fraud, plagiarism, and other forms of academic misconduct are violations of the institution's policies and may result in disciplinary action, including suspension or expulsion**.**