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

SYLLABUS

GENERAL INFORMATION

Course Title:	CompTIA CySA+
Code:	CS0-003
Contact Hours:	40
Academic Term:	TBA

COURSE DESCRIPTION

The CompTIA Cybersecurity Analyst (CySA+) course is a comprehensive program designed to equip participants with the essential skills and knowledge required to become proficient cybersecurity analysts. This course prepares students to effectively identify and address vulnerabilities in the information security environment, ensuring the protection and integrity of network and system operations.

Upon completion of this course, students will be prepared to sit for the CompTIA CySA+ certification exam, which is recognized globally as a standard for cybersecurity analytical proficiency. This course is ideal for IT professionals looking to advance their career in cybersecurity, system and network analysts, and anyone interested in understanding the complexities of securing information systems.

GENERAL OBJECTIVES

Throughout the course, students will delve into real-world scenarios that simulate complex cybersecurity challenges. The curriculum covers:

- **Threat and Vulnerability Management:** Learn to identify and evaluate vulnerabilities, conduct environmental reconnaissance, and utilize threat data to prepare for and respond to incidents.
- **Software and Systems Security:** Gain knowledge on the importance of software security, including best practices in secure software deployment and the lifecycle management of software.
- **Security Operations and Monitoring:** Focus on the detection, response, and recovery from network and system incidents. Learn to use tools for continuous

security monitoring and analytics to identify anomalies that could indicate a cybersecurity incident.

- **Incident Response:** Understand the key steps in planning and conducting an effective incident response, including forensics handling and legal considerations to support recovery and continuity.
- **Compliance and Assessment:** Study frameworks and policies for cybersecurity, including risk mitigation strategies and the role of governance, risk, and compliance (GRC) in cybersecurity.

COURSE CONTENT

Lesson 1: Understanding Vulnerability Response, Handling, and Management

Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts

Lesson 3: Explaining Important System and Network Architecture Concepts

Lesson 4: Understanding Process Improvement in Security Operations

Lesson 5: Implementing Vulnerability Scanning Methods

Lesson 6: Performing Vulnerability Analysis

Lesson 7: Communicating Vulnerability Information

Lesson 8: Explaining Incident Response Activities

Lesson 9: Demonstrating Incident Response Communication

Lesson 10: Applying Tools to Identify Malicious Activity

Lesson 11: Analyzing Potentially Malicious Activity

Lesson 12: Understanding Application Vulnerability Assessment

Lesson 13: Exploring Scripting Tools and Analysis Concepts

Lesson 14: Understanding Application Security and Attack Mitigation Best Practices

Lesson 1: Understanding Vulnerability Response, Handling, and Management

Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts

Lesson 3: Explaining Important System and Network Architecture Concepts

Lesson 4: Understanding Process Improvement in Security Operations

Lesson 5: Implementing Vulnerability Scanning Methods

Lesson 6: Performing Vulnerability Analysis

Lesson 7: Communicating Vulnerability Information

Lesson 8: Explaining Incident Response Activities

Lesson 9: Demonstrating Incident Response Communication

Lesson 10: Applying Tools to Identify Malicious Activity

Lesson 11: Analyzing Potentially Malicious Activity

Lesson 12: Understanding Application Vulnerability Assessment

Lesson 13: Exploring Scripting Tools and Analysis Concepts

Lesson 14: Understanding Application Security and Attack Mitigation Best Practices

EVALUATION CRITERIA

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

Assignments are always due in class on the day designated. You are responsible for any work lost due to technical problems, etc. Late papers will lose a letter grade for each day that they are late. Any exceptions must be properly documented and discussed in advance for an extension to be arranged.

EDUCATIONAL RESOURCES

Marchant, G. (2023). The Official CompTIA CySA+ Guide (CS0-003). *CompTIA*, Inc. Downers Grove, Illinois.
ISBN: 978-1-64274-485-9

NOTES

• ***Reasonable Accommodation*:** Any student who requires a reasonable accommodation should do the request at the beginning of the course or as soon as he / she acquires knowledge of what it requires, through the Professor in charge and this notifying the Academic Director.

• ***Honesty, fraud, plagiarism:*** The lack of honesty, fraud, plagiarism and / or any other inappropriate behavior in relation to the student's academic performance constitute violations of the Institution's Catalog, its Rules of Conduct and Student Duties. Major infractions, as determined by the Catalog, may result in the suspension of the Institution for a definite time or permanent expulsion as stipulated in the Norms of Conduct and Duties of the Student.