Password Technical College
44 Calle Dr. Santiago Veve
San Germán, PR 00683
http://passwordtech.edu20.org

SYLLABUS

GENERAL INFORMATION

Course Title:	CompTIA Security +
Code:	SY0-601
Contact Hours:	40
Term:	TBA

COURSE DESCRIPTION

The CompTIA Security+ certification course is an essential program for individuals aiming to pursue a career in information security. This globally recognized course provides a comprehensive overview of fundamental security principles and practices, preparing participants to handle a variety of cybersecurity roles effectively. The course is designed to ensure students gain practical security problem-solving skills, encompassing core topics necessary for any cybersecurity role.

OBJECTIVE

Upon successful completion of this course, students should be able to:

Identify the fundamental concepts of computer security, identify security threats and vulnerabilities, examine network security, manage application, data, and host security, identify access control and account management security measures, identify compliance and operational security measures, manage risk, manage security incidents, develop business continuity and disaster recovery plans. The CompTIA® Security+® courses are designed to help you prepare for the SY0-601 exam.

SKILLS DISTRIBUTION

Lesson 1: Comparing Security Roles and Security Controls

Lesson 2: Explaining Threat Actors and Threat Intelligence

Lesson 3: Performing Security Assessments

Lesson 4: Identifying Social Engineering and Malware

Lesson 5: Summarizing Basic Cryptographic Concepts

Lesson 6: Implementing Public Key Infrastructure

Lesson 7: Implementing Authentication Controls

Lesson 8: Implementing Identity and Account Management Controls

Lesson 9: Implementing Secure Network Designs

Lesson 10: Implementing Network Security Appliances

Lesson 11: Implementing Secure Network Protocols

Lesson 12: Implementing Host Security Solutions

Lesson 13: Implementing Secure Mobile Solutions

Lesson 14: Summarizing Secure Application Concepts

Lesson 15: Implementing Secure Cloud Solutions

Lesson 16: Explaining Data Privacy and Protection Concepts

Lesson 17: Performing Incident Response

Lesson 18: Explaining Digital Forensics

Lesson 19: Summarizing Risk Management Concepts

Lesson 20: Implementing Cybersecurity Resilience

Lesson 21: Explaining Physical Security

EVALUATION CRITERIA

CRITERIA	Grade total
1 Mid-Term Exam	100
1 Final Exam	100
Quizzes	100
Homework or Assessments	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

Neo LMS (2020). CompTIA Security +. *passwordtech.edu20*.
https://passwordtech.edu20.org/

Pengelly, J. (2020). The Official CompTIA Security + Student Guide (Exam SY0-601). eBook CompTIA. Downers Grove, Illinois
ISBN: 978-1-64274-328-9

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.