CompTIA Security+ SY0-701 Exam Prep

Florida Cybersecurity Training Program

Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course / Cyber Skills Exercise Dates: 1 July – August 30, 2024

Cyber Skills Exercise Times: N/A

Duration: 8 weeks + 1 test week

Estimated Time Commitment: 20 hours per week for individuals with pre-requisite knowledge; 20+ hours per week for individuals with no prior professional experience or technical education.

Instructional Hours: 40 contact hours

Delivery Format: Asynchronous online with weekly instructor Zoom sessions on Mondays.

Target Audience: Early career IT practitioners with a security function 1+-years' experience recommended, college graduates with hands-on cybersecurity course backgrounds, uniformed and civilian personnel subject to DoD Regulation 8570/8140.

Required Prerequisites / Background: Recommended (CompTIA) minimum 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts and networking. Network+ certification or equivalent is highly recommended.

CEU's: 4.0, **CPE's:** 48

Course Instructor

Instructor	Email Address
Guy Garrett, M.S., M.B.A.	ggarrett@uwf.edu

Course Description

This course has one purpose – preparing you to take and pass the CompTIA Security+ exam. The goal is mastering concepts, terminology, processes, and procedures to the point that you can accurately apply them to various situations.

What is Sec+?
Sec+ is a global industry certification that validates the foundational cybersecurity skills necessary to perform core security functions and pursue an IT security career.

What should a successful candidate know and be able to do?

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

How to succeed in this course.

- Manage your time. Most students average 20-30 hours/week for exam prep.
- Actively engage your instructor.
- Do the labs and watch the demonstrations. This test is performance-based. Hands-on work is the key to conquering situation-based questions.

CompTIA Exam Objectives

Domain #	Domain	% Weight on Exam
1	General Security Concepts	12
2	Threats, Vulnerabilities, and Mitigations	22
3	Security Architecture	18
4	Security Operations	28
5	Security Program Management & Oversight	20

NIST NICE Cybersecurity Workforce Framework Mapping

The course addresses cybersecurity work roles as identified in NIST's Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

Cybersecurity Work Roles and Categories:
Operate and Maintain

- Technical Support Specialist (411)
- System Administrator (451)
- Network Operations Specialist (441)
- Systems Security Analyst (461)

Course Information

Materials

- Course organization, including assignments, grading, and instructor-student communication will be done through the Canvas learning management system (LMS).
- This course uses a variety of materials, including the official curriculum from CompTIA-TestOut. Students will be given access codes and instructions on the first day of class to access these resources and connect to the correct class.

Technical Specifications

- Reliable high speed Internet connection | Computer with up-to-date browser.
- Students should have a computer with microphone, speakers, camera (optional), capable of running Zoom sessions.

Student Accessibility Resources:

If you have a disability that impacts your full participation in this course, please email Student Accessibility Resources at 850.474.2387 or by email, sar@uwf.edu.

Grading

This course is designed for workforce development and focuses on concept and task mastery learning. Students are required to complete 70% of all assigned material in order to pass the course and receive a digital badge. **Doing only 70% of the assignments is not sufficient to pass the certification exam.**

Assignments are rated based on the following scale.

Rating	Requirements	Progress
4	Scored 90% or higher on the assignment	Likely to pass cert exam
3	Scored 80%-89% on the assignment	Possibly pass cert exam
2	Scored 70%-79% on the assignment	Requires remediation to pass cert exam
1	Scored >70% on the assignment	Unlikely to pass cert exam
0	Failed to complete the assignment	Will not pass cert exam

Course Overview / Schedule

Course Information

Assessments: PBQs, Labs, Practice Exams, Certification Exam

Domain 1.0 General Security Concepts
1.1 Compare and contrast various types of security controls.
1.2 Summarize fundamental security concepts.
1.3 Explain the importance of change management processes and the impact to security.

1.4 Explain the importance of using appropriate cryptographic solutions.

Domain 2.0 Threats, Vulnerabilities, and Mitigations
2.1 Compare and contrast common threat actors and motivations.
2.2 Explain common threat vectors and attack surfaces.
2.3 Explain various types of vulnerabilities.
2.4 Given a scenario, analyze indicators of malicious activity.
2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

Domain 3.0 Security Architecture
3.1 Compare and contrast security implications of different architecture models.
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.
3.3 Compare and contrast concepts and strategies to protect data.
3.4 Explain the importance of resilience and recovery in security.

Domain 4.0 Security Operations
4.1 Given a scenario, apply common security techniques to computing resources.
4.2 Explain the security implications of proper hardware, software, and data asset management.
4.3 Explain various activities associated with vulnerability management.
4.4 Explain security alerting and monitoring concepts and tools.
4.5 Given a scenario, modify enterprise capabilities to enhance security.
4.6 Given a scenario, implement and maintain identity and access management.
4.7 Explain the importance of automation and orchestration related to security operations.
4.8 Explain appropriate incident response activities.
4.9 Given a scenario, use data sources to support an investigation.

Domain 5.0 Security Program Management and Oversight
5.1 Summarize elements of effective security governance.
5.2 Explain elements of the risk management process.
5.3 Explain the processes associated with third-party risk assessment and management.
5.4 Summarize elements of effective security compliance.
5.5 Explain types and purposes of audits and assessments.
5.6 Given a scenario, implement security awareness practices.

Course Outline

Week #	Lessons
1	Lesson 1: Summarize Fundamental Security Concepts Lesson 2: Compare Threat Types
2	Lesson 3: Explain Cryptographic Solutions Lesson 4: Implement Identity and Access Management
3	Lesson 5: Secure Enterprise Network Architecture Lesson 6: Secure Cloud Network Architecture
4	Lesson 7: Explain Resiliency and Site Security Concepts Lesson 8: Explain Vulnerability Management
5	Lesson 9: Evaluate Network Security Capabilities Lesson 10: Assess Endpoint Security Capabilities.

6	Lesson 11: Enhance Application Security Capabilities Lesson 12: Explain Incident Response and Monitoring Concepts
7	Lesson 13: Analyze Indicators of Malicious Activity Lesson 14: Summarize Security Governance Concepts
8	Lesson 15: Explain Risk Management Processes Lesson 16: Summarize Data Protection and Compliance Concepts.
9	Exam Week