CompTIA Security+ Certification (SY0-601)

Overview

The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents

Prerequisite Comments

A+, Network+

Target Audience

This course is designed for information technology (IT) professionals who have networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; familiarity with other operating systems, such as macOS®, Unix®, or Linux®; and who want to further a career in IT by acquiring foundational knowledge of security topics or using CompTIA Security+ as the foundation for advanced security certifications or career roles.
This course is also designed for students who are seeking the CompTIA Security+ certification and who want to prepare for the CompTIA Security+ SY0-601 Certification Exam.

Course Objectives

Compare and contrast different types of social engineering techniques.
Given a scenario, analyze potential indicators to determine the type of attack.
Given a scenario, analyze potential indicators associated with application and network attacks.
Explain different threat actors, vectors, and intelligence sources.
Explain the security concerns associated with various types of vulnerabilities.
Summarize the techniques used in security assessments.
Explain the techniques used in penetration testing.
Explain the importance of security concepts in an enterprise environment.
Summarize virtualization and cloud computing concepts and authentication and authorication design concepts.
Summarize secure application development,deployment, and automation concepts.
Given a scenario, implement cybersecurity resilience.
Explain the security implications of embedded and specialized systems.
Explain the importance of physical security controls.
Summarize the basics of cryptographic concepts.
Given a scenario, implement secure protocols.
Given a scenario, implement host or application security solutions and secure network designs.
Given a scenario, install and configure wireless security settings and implement secure mobile solutions.
Given a scenario, apply cybersecurity solutions to the cloud.
Given a scenario, implement identity and account management controls and authentication and authorization solutions.
Given a scenario, implement public key infrastructure.
Given a scenario, use the appropriate tool to assess organizational security.
Summarize the importance of policies, processes, and procedures for incident response.
Given an incident, utilize appropriate data sources to support an investigation.

Given an incident, apply mitigation techniques or controls to secure an environment.
Explain the key aspects of digital forensics.
Compare and contrast various types of controls.
Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.
Explain the importance of policies to organizational security.
Summarize risk management processes and concepts.
Explain privacy and sensitive data concepts in relation to security.

Course Outline

1 - Threats, Attacks, and Vulnerabilities

Compare and contrast different types of social engineering techniques.
Given a scenario, analyze potential indicators to determine the type of attack.
Given a scenario, analyze potential indicators associated with application attacks.
Given a scenario, analyze potential indicators associated with network attacks.
Explain different threat actors, vectors, and intelligence sources.
Explain the security concerns associated with various types of vulnerabilities.
Summarize the techniques used in security assessments.
Explain the techniques used in penetration testing.

2 - Architecture and Design

Explain the importance of security concepts in an enterprise environment.
Summarize virtualization and cloud computing concepts.
Summarize secure application development, deployment, and automation concepts.
Summarize authentication and authorization design concepts.
Given a scenario, implement cybersecurity resilience.
Explain the security implications of embedded and specialized systems.
Explain the importance of physical security controls.
Summarize the basics of cryptographic concepts.

3 - Implementation

Given a scenario, implement secure protocols.
Given a scenario, implement host or application security solutions.
Given a scenario, implement secure network designs.
Given a scenario, install and configure wireless security settings.
Given a scenario, implement secure mobile solutions.
Given a scenario, apply cybersecurity solutions to the cloud.
Given a scenario, implement identity and account management controls.
Given a scenario, implement authentication and authorization solutions.
Given a scenario, implement public key infrastructure.

4 - Operations and Incident Response

Given a scenario, use the appropriate tool to assess organizational security.
Summarize the importance of policies, processes, and procedures for incident response.
Given an incident, utilize appropriate data sources to support an investigation.
Given an incident, apply mitigation techniques or controls to secure an environment.
Explain the key aspects of digital forensics.

5 - Governance, Risk, and Compliance

Compare and contrast various types of controls.
Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.
Explain the importance of policies to organizational security.
Summarize risk management processes and concepts.
Explain privacy and sensitive data concepts in relation to security.

Related Courses, Certifications, Exams

- CompTIA Cybersecurity Analyst (CySA+) Certification (Exam CS0-002)