Course Outline

ProTech Professional Technical Services, Inc.

The Official CompTIA Security+ (Exam SY0-601)

Course Summary

Description

The Official CompTIA Security+ Study Guide (SY0-601) has been developed by CompTIA for the CompTIA certification candidate. Rigorously evaluated by third party subject matter experts to validate adequate coverage of the Security+ exam objectives, the Official CompTIA Security+ Study Guide teaches the essential skills and information required for the CompTIA certification exam (SY0-601).

Objectives

Successful candidates will have the knowledge 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.

Topics

- Comparing Security Roles and Security Controls
- Explaining Threat Actors and Threat Intelligence
- Performing Security Assessments
- Identifying Social Engineering and Malware
- Summarizing Basic Cryptographic Concepts
- Implementing Public Key Infrastructure
- Implementing Authentication Controls
- Implementing Identity and Account Management Controls
- Implementing Secure Network Designs
- Implementing Network Security Appliances
- Implementing Secure Network Protocols
- Implementing Host Security Solutions
- Implementing Secure Mobile Solutions
- Summarizing Secure Application Concepts
- Implementing Secure Cloud Solutions
- Explaining Data Privacy and Protection Concepts
- Performing Incident Response
- Explaining Digital Forensics
- Summarizing Risk Management Concepts
- Implementing Cybersecurity Resilience
- Explaining Physical Security

Audience

This course is targeted toward the information technology (IT) professional who has 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 wants to further a career in IT by acquiring foundational knowledge of security topics; preparing for the CompTIA Security+ certification examination; or using Security+ as the foundation for advanced security certifications or career roles.

Prerequisites

To ensure your success in this course, you should have basic Windows user skills and a fundamental understanding of computer and networking concepts. CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months' experience in networking, including configuring security parameters, are strongly recommended.

Duration

Five days

Course Outline

The Official CompTIA Security+ (Exam SY0-601)

Course Outline

I. Comparing Security Roles and Controls
- A. Compare and Contrast Information Security Roles
- B. Compare and Contrast Security Control and Framework Types

II. Explaining Threat Actors and Threat Intelligence
- A. Explain Threat Actor Types and Attack Vectors
- B. Explain Threat Intelligence Sources

III. Performing Security Assessments
- A. Assess Organizational Security with Network Reconnaissance Tools
- B. Explain Security Concerns with General Vulnerability Types
- C. Summarize Vulnerability Scanning Techniques
- D. Explain Penetration Testing Concepts

IV. Identify Social Engineering and Malware
- A. Compare and Contrast Social Engineering Techniques
- B. Analyze Indicators of Malware-Based Attacks

V. Summarizing Basic Cryptographic Concepts
- A. Compare and Contrast Cryptographic Ciphers
- B. Summarize Cryptographic Modes of Operation
- C. Summarize Cryptographic Use Cases and Weaknesses
- D. Summarize Other Cryptographic Technologies

VI. Implementing Public Key Infrastructure
- A. Implement Certificates and Certificate Authorities
- B. Implement PKI Management

VII. Implementing Authorization Control
- A. Summarize Authentication Design Concepts
- B. Implement Knowledge-Based Authentication
- C. Implement Authentication Technologies
- D. Summarize Biometrics Authentication Concepts

VIII. Implementing Identity and Account Management Controls
- A. Implement Identity and Account Types
- B. Implement Account Policies
- C. Implement Authorization Solutions
- D. Explain the Importance of Personnel Policies

IX. Implementing Secure Network Designs
- A. Implement Secure Network Designs
- B. Implement Secure Switching and Routing
- C. Implement Secure Wireless Infrastructure
- D. Implement Load Balancers

X. Implementing Network Security Appliances
- A. Implement Firewalls and Proxy Servers
- B. Implement Network Security Monitoring

XI. Implementing Secure Network Protocols
- A. Implement Secure Network Operations Protocols
- B. Implement Secure Application Protocols
- C. Implement Secure Remote Access Protocols

XII. Implementing Host Security Solutions
- A. Implement Secure Firmware
- B. Implement Endpoint Security
- C. Explain Embedded System Security Implications

XIII. Implementing Secure Mobile Solutions
- A. Implement Mobile Device Management
- B. Implement Secure Mobile Device Connections

XIV. Summarizing Secure Application Concepts
- A. Analyze Indicators of Application Attacks
- B. Analyze Indicators of Web Application Attacks
- C. Summarize Secure Coding Practices
- D. Implement Secure Script Environments
- E. Summarize Deployment and Automation Concepts

XV. Implementing Secure Cloud Solutions
- A. Summarize Secure cloud and Virtualization Services
- B. Apply Cloud Security Solutions
- C. Summarize Infrastructure as Code Concepts

XVI. Explaining Data Privacy and Protection Concepts
- A. Explain Privacy and Data Sensitivity Concepts
- B. Explain Privacy and Data Protection Controls

Course Outline (cont)

XVII. Performing Incident Response
- A. Summarize Incident Response Procedures
- B. Utilize Appropriate Data Sources for Incident Response
- C. Apply Mitigation Controls

XVIII. Explaining Digital Forensics
- A. Explain Key Aspects of Digital Forensics Documentation
- B. Explain Key Aspects of Digital Forensics Evidence Acquisition

XIX. Summarizing Risk Management Concepts
- A. Explain Risk Management Processes and Concepts
- B. Explain Business Impact and Analysis Concepts

XX. Implementing Cybersecurity Resilience
- A. Implement Redundancy Strategies
- B. Implement Backup Strategies
- C. Implement Cybersecurity Resiliency Strategies

XXI. Explaining Physical Security
- A. Explain the Importance of Physical Site Security Controls
- B. Explain the Importance of Physical Host Security Controls