CompTIA Security+ Certification (Exam SY0-601)

Summary

Length: 40 hours Level: Experienced

This course maps to the CompTIA Security+ certification exam (SK0-601) and establishes the core knowledge required of any cybersecurity role, as well as providing a springboard to intermediate-level cybersecurity jobs. This course emphasizes both the practical and hands-on ability to identify and address security threats, attacks and vulnerabilities. CompTIA Security+ is a globally trusted, vendor-neutral certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career. CompTIA Security+ is also a DoD Approved 8570 Baseline Certification and this course meets DoD 8140/8570 Training requirements This course may earn a Credly Badge.

Learning Objectives

In this course you will:

Prepare for the CompTIA Security+ exam
Confidently explain and define an array of security vulnerabilities
Navigate the complexities of secure system and network design
Explore the defensive measures like PKI, firewalls and IDS
Implement robust identity management and access control

Course Outline

1. Comparing Security Roles and Controls

   Topic 1A- Compare and Contrast Information Security Roles
   Topic 1B- Compare and Contrast Security Control and Framework Types

2. Explaining Threat Actors and Threat Intelligence

   Topic 2A- Explain Threat Actor Types and Attack Vectors

3. Performing Security Assessments

   Topic 3A- Assess Organizational Security with Network Reconnaissance Tools
   Topic 3B- Explain Security Concerns with General Vulnerability Types
   Topic 3C- Summarize Vulnerability Scanning Techniques
   Topic 3D- Explain Penetration Testing Concepts

4. Identifying Social Engineering and Malware

   Topic 4A- Compare and Contrast Social Engineering Techniques
   Topic 4B- Analyze Indicators of Malware-Based Attacks

5. Summarizing Basic Cryptographic Concepts

   Topic 5A- Compare and Contrast Cryptographic Ciphers
   Topic 5B- Summarize Cryptographic Modes of Operation
   Topic 5C- Summarize Cryptographic Use Cases and Weaknesses
   Topic 5D- Summarize Other Cryptographic Technologies

6. Implementing Public Key Infrastructure

Topic 6A- Implement Certificates and Certificate Authorities
Topic 6B- Implement PKI Management

7. Implementing Authentication Controls

Topic 7A- Summarize Authentication Design Concepts
Topic 7B- Implement Knowledge-Based Authentication
Topic 7C- Implement Authentication Technologies
Topic 7D- Summarize Biometrics Authentication Concepts

8. Implementing Identity and Account Management Controls

Topic 8A- Implement Identity and Account Types
Topic 8B- Implement Account Policies
Topic 8C- Implement Authorization Solutions
Topic 8D- Explain the Importance of Personnel Policies

9. Implementing Secure Network Designs

Topic 9A- Implement Secure Network Designs
Topic 9B- Implement Secure Switching and Routing
Topic 9C- Implement Secure Wireless Infrastructure
Topic 9D- Implement Load Balancers

10. Implementing Network Security Appliances

Topic 10A- Implement Firewalls and Proxy Servers
Topic 10B- Implement Network Security Monitoring
Topic 10C- Summarize the Use of SIEM

11. Implementing Secure Network Protocols

Topic 11A- Implement Secure Network Operations Protocols
Topic 11B- Implement Secure Application Protocols
Topic 11C- Implement Secure Remote Access Protocols

12. Implementing Host Security Solutions

Topic 12A- Implement Secure Firmware
Topic 12B- Implement Endpoint Security
Topic 12C- Explain Embedded System Security Implications

13. Implementing Secure Mobile Solutions

Topic 13A- Implement Mobile Device Management
Topic 13B- Implement Secure Mobile Device Connections

14. Summarizing Secure Application Concepts

Topic 14A- Analyze Indicators of Application Attacks
Topic 14B- Analyze Indicators of Web Application Attacks
Topic 14C- Summarize Secure Coding Practices
Topic 14D- Implement Secure Script Environments
Topic 14E- Summarize Deployment and Automation Concepts

15. Implementing Secure Cloud Solutions

Topic 15A- Summarize Secure Cloud and Virtualization Services
Topic 15B- Apply Cloud Security Solutions
Topic 15C- Summarize Infrastructure as Code Concepts

16. Explaining Data Privacy and Protection Concepts

    Topic 16A- Explain Privacy and Data Sensitivity Concepts
    Topic 16B- Explain Privacy and Data Protection Controls

17. Performing Incident Response

    Topic 17A- Summarize Incident Response Procedures
    Topic 17B- Utilize Appropriate Data Sources for Incident Response
    Topic 17C- Apply Mitigation Controls

18. Explaining Digital Forensics

    Topic 18A- Explain Key Aspects of Digital Forensics Documentation
    Topic 18B- Explain Key Aspects of Digital Forensics Evidence Acquisition

19. Summarizing Risk Management Concepts

    Topic 19A- Explain Risk Management Processes and Concepts

20. Implementing Cybersecurity Resilience

    Topic 20A- Implement Redundancy Strategies
    Topic 20B- Implement Backup Strategies
    Topic 20C- Implement Cybersecurity Resiliency Strategies

21. Explaining Physical Security

    Topic 21A- Explain the Importance of Physical Site Security Controls
    Topic 21B- Explain the Importance of Physical Host Security Controls

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.

Prerequisites

A+, Network+