CompTIA Security+ Certification - 2019 Update

Overview
In this course, students will build on their knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.

Prerequisite Comments
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.

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+ SY0-501 Certification Exam.

Course Objectives
In this course, students will use fundamental security principles to install and configure cybersecurity controls and participate in incident response and risk mitigation.

Students will:
- Compare and contrast attacks.
- Compare and contrast security controls.
- Use security assessment tools.
- Explain basic cryptography concepts.
- Implement a public key infrastructure.
- Implement identity and access management controls.
- Manage access services and accounts.
- Implement a secure network architecture.
- Install and configure security appliances.
- Install and configure wireless and physical access security.
- Deploy secure host, mobile, and embedded systems.
- Implement secure network access protocols.
- Implement secure network applications.
- Explain risk management and disaster recovery concepts.
- Describe secure application development concepts.
- Explain organizational security concepts.

Course Outline

Comparing and Contrasting Attacks

Compare and Contrast Information Security Roles
Explain Threat Actor Types
Compare and Contrast Social Engineering Attack Types
Determine Malware Types

Comparing and Contrasting Security Controls

Compare and Contrast Security Control and Framework Types
Follow Incident Response Procedures

Assessing Security Posture with Software Tools

Explain Penetration Testing Concepts
Assess Security Posture with Topology Discovery Software Tools
Assess Security Posture with Fingerprinting and Sniffing Software Tools
Assess Security Posture with Vulnerability Scanning Software Tools

Explaining Basic Cryptography Concepts

Compare and Contrast Basic Concepts of Cryptography
Explain Hashing and Symmetric Cryptographic Algorithms
Explain Asymmetric Cryptographic Algorithms

Implementing a Public Key Infrastructure

Implement Certificates and Certificate Authorities
Implement PKI Management

Implementing Identity and Access Management Controls

Compare and Contrast Identity and Authentication Concepts
Install and Configure Authentication Protocols
Implement Multifactor Authentication

Managing Access Services and Accounts

Install and Configure Authorization and Directory Services
Implement Access Management Controls
Differentiate Account Management Practices
Implement Account Auditing and Recertification
Implementing a Secure Network Architecture
Implement Secure Network Architecture Concepts
Install and Configure a Secure Switching Infrastructure
Install and Configure Network Access Control
Install and Configure a Secure Routing and NAT Infrastructure

Installing and Configuring Security Appliances
Install and Configure Firewalls and Proxies
Install and Configure Load Balancers
Install and Configure Intrusion Detection/Prevention Systems
Install and Configure Data Loss Prevention (DLP) Systems
Install and Configure Logging and SIEM Systems

Installing and Configuring Wireless and Physical Access Security
Install and Configure a Wireless Infrastructure
Install and Configure Wireless Security Settings
Explain the Importance of Physical Security Controls

Deploying Secure Host, Mobile, and Embedded Systems
Implement Secure Hardware Systems Design
Implement Secure Host Systems Design
Implement Secure Mobile Device Systems Design
Implement Secure Embedded Systems Design

Implementing Secure Network Access Protocols
Implement Secure Network Operations Protocols
Implement Secure Remote Access Protocols
Implement Secure Remote Administration Protocols

Implementing Secure Network Applications
Implement Secure Web Services
Implement Secure Communications Services
Summarize Secure Virtualization Infrastructure
Summarize Secure Cloud Services

Explaining Risk Management and Disaster Recovery Concepts
Explain Risk Management Processes and Concepts
Explain Resiliency and Automation Strategies
Explain Disaster Recovery and Continuity of Operation Concepts
Summarize Basic Concepts of Forensics
Summarizing Secure Application Development Concepts

Explain the Impact of Vulnerability Types
Summarize Secure Application Development Concepts

Explaining Organizational Security Concepts

Explain the Importance of Security Policies
Implement Data Security and Privacy Practices
Explain the Importance of Personnel Management

Related Courses, Certifications, Exams

- CompTIA Network+ Certification
- CompTIA A+ Certification (Exams 220-1001 and 220-1002)
- CompTIA Cybersecurity Analyst (CySA+) Certification
- CompTIA Penetration Tester+ (PenTest+) Certification