CompTIA® Security+™

Duration: 5 Days
Method: Instructor-Led Training (ILT)

Certification: *CompTIA Security+* — ***Exam:*** *SY0-501*

Course Description

This course is designed to help attendees prepare for the certification exam. Attendees will implement and monitor security on networks, applications, and operating systems, and respond to security breaches.

Target Audience

This course is intended for:

- Information Technology (IT) professionals who want to either:
  - Further their IT career by acquiring a foundational knowledge of security topics
  - Prepare for the certification exam
  - Use this course as the foundation for advanced security certifications or career roles

Prerequisites

To attend this course, candidates must have the following:

- Basic Windows® user skills and a fundamental understanding of computer and networking concepts. To obtain this level of skills and knowledge, complete the following courses:
  - CompTIA A+®
  - CompTIA Network+®
- At least two (2) years of experience in IT administration with a security focus.

Exam Details

Exam Title:	• CompTIA Security+
Exam Code:	• SY0-501
Length of Exam:	• 90 minutes
Number of Questions:	• 90 max.
Passing Score:	• 750 out of 900
Question Format:	• Multiple Choice and Performance Based Questions

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Identify the fundamental concepts of computer security.
- Identify security threats and vulnerabilities.
- Examine network security.
- Manage application, data and host security.
- Identify access control and account management security measures.
- Manage certificates.
- Identify compliance and operational security measures.
- Manage risk.
- Manage security incidents.
- Develop business continuity and disaster recovery plans.

Course Topics

Module 1: Security Fundamentals

- Information Security Cycle
- Information Security Controls
- Authentication Methods
- Cryptography Fundamentals
- Security Policy Fundamentals

Module 2: Identifying Security Threats and Vulnerabilities

- Social Engineering
- Malware
- Physical Threats and Vulnerabilities
- Software-Based Threats
- Network-Based Threats
- Wireless Threats and Vulnerabilities
- Physical Threats and Vulnerabilities

Module 3: Managing Data, Application, and Host Security

- Manage Data Security
- Manage Application Security
- Manage Device and Host Security
- Manage Mobile Security

Module 4: Implementing Network Security

- Configure Security Parameters on Network Devices and Technologies
- Network Design Elements and Components
- Implement Networking Protocols and Services
- Apply Secure Network Administration Principles
- Secure Wireless Traffic

Course Topics *Continued*

Module 5: Implementing Access Control, Authentication, and Account Management

- Access Control and Authentication Services
- Implement Account Management Security Controls

Module 6: Managing Certificates

- Install a Certificate Authority (CA) Hierarchy
- Enrol Certificates
- Secure Network Traffic by Using Certificates
- Renew Certificates
- Revoke Certificates
- Back Up and Restore Certificates and Private Keys
- Restore Certificates and Private Keys

Module 7: Implementing Compliance and Operational Security

- Physical Security
- Legal Compliance
- Security Awareness and Training
- Integrate Systems and Data with Third Parties

Module 8: Risk Management

- Risk Analysis
- Implement Vulnerability Assessment Tools and Techniques
- Scan for Vulnerabilities
- Mitigation and Deterrent Techniques

Module 9: Troubleshooting and Managing Security Incidents

- Respond to Security Incidents
- Recover from a Security Incident

Module 10: Business Continuity and Disaster Recovery Planning

- Business Continuity
- Plan for Disaster Recovery
- Execute Disaster Recovery Plans and Procedures

LABS INCLUDED