CompTIA® Security+ Certification (Exam SY0-501)

Ctrl+ Click here to enquire about this course:

Course Specifications

Course length: 4.0 day(s)

Overview:

The Official CompTIA® Security+® (Exam SY0-501) course is the primary curriculum you will need to take if your job responsibilities include securing network services, devices, and traffic in your organization. You can also take this course to prepare for the CompTIA Security+ certification examination. In this course, you will build on your 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.

Course Objectives:

In this course, you will implement, monitor, and troubleshoot infrastructure, application, information, and operational security.

You will:

In this course, you will implement information security across a variety of different contexts.

You will:

- Identify the fundamental components of information security.
- Analyze risk.
- Identify various threats to information security.
- Conduct security assessments to detect vulnerabilities.
- Implement security for hosts and software.
- Implement security for networks.
- Manage identity and access.
- Implement cryptographic solutions in the organization.
- Implement security at the operational level.
- Address security incidents.
- Ensure the continuity of business operations in the event of an incident.

Target Student:

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 Mac OS X®, Unix, or Linux; and who wants to further a career in IT by acquiring foundational knowledge of security topics; prepare for the CompTIA Security+ certification examination; or use Security+ as the foundation for advanced security certifications or career roles.

CompTIA® Security+ Certification (Exam SY0-501)

Ctrl+ Click here to enquire about this course:

Prerequisites:

To ensure your success in this course, you should possess 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. Students can obtain this level of skill and knowledge by taking any of the following courses:

- *CompTIA® A+®: A Comprehensive Approach (Exams 220-901 and 220-902)*
- *CompTIA® Network+® (Exam N10-006)*

Additional introductory courses or work experience in application development and programming, or in network and operating system administration for any software platform or system, are helpful but not required.

Course Objectives

Upon successful completion of this course, students 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 a BCP and DRP.

CompTIA® Security+ Certification (Exam SY0-501)

Ctrl+ Click here to enquire about this course:

Course Content

Lesson 1: Identifying Security Fundamentals

Topic A: Identify Information Security Concepts

Topic B: Identify Basic Security Controls

Topic C: Identify Basic Authentication and Authorization Concepts

Topic D: Identify Basic Cryptography Concepts

Lesson 2: Analyzing Risk

Topic A: Analyze Organizational Risk

Topic B: Analyze the Business Impact of Risk

Lesson 3: Identifying Security Threats

Topic A: Identify Types of Attackers

Topic B: Identify Social Engineering Attacks

Topic C: Identify Malware

Topic D: Identify Software-Based Threats

Topic E: Identify Network-Based Threats

Topic F: Identify Wireless Threats

Topic G: Identify Physical Threats

Lesson 4: Conducting Security Assessments

Topic A: Identify Vulnerabilities

Topic B: Assess Vulnerabilities

Topic C: Implement Penetration Testing

Lesson 5: Implementing Host and Software Security

Topic A: Implement Host Security

Topic B: Implement Cloud and Virtualization Security

Topic C: Implement Mobile Device Security

Topic D: Incorporate Security in the Software Development Lifecycle

Lesson 6: Implementing Network Security

Topic A: Configure Network Security Technologies

Topic B: Secure Network Design Elements

Topic C: Implement Secure Networking Protocols and Services

Topic D: Secure Wireless Traffic

Lesson 7: Managing Identity and Access

Topic A: Implement Identity and Access Management
Topic B: Configure Directory Services
Topic C: Configure Access Services
Topic D: Manage Accounts

Lesson 8: Implementing Cryptography

Topic A: Identify Advanced Cryptography Concepts
Topic B: Select Cryptographic Algorithms
Topic C: Configure a Public Key Infrastructure
Topic D: Enroll Certificates
Topic E: Back Up and Restore Certificates and Private Keys
Topic F: Revoke Certificates

Lesson 9: Implementing Operational Security

Topic A: Evaluate Security Frameworks and Guidelines
Topic B: Incorporate Documentation in Operational Security
Topic C: Implement Security Strategies
Topic D: Manage Data Security Processes
Topic E: Implement Physical Controls

Lesson 10: Addressing Security Incidents

Topic A: Troubleshoot Common Security Issues
Topic B: Respond to Security Incidents
Topic C: Investigate Security Incidents

Lesson 11: Ensuring Business Continuity

Topic A: Select Business Continuity and Disaster Recovery Processes
Topic B: Develop a Business Continuity Plan