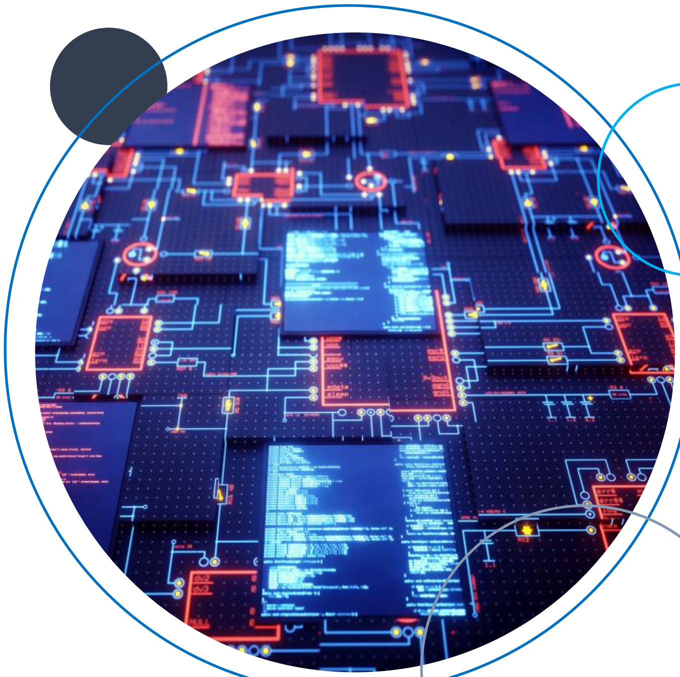
OVERVIEW

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.

This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (Exam SY0-501) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of computer security. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your computer security skill set so that you can confidently perform your duties in any security-related role.

XTREMELABS



COMPTIA SECURITY+

COURSE DURATION: 5 DAYS

COURSE OBJECTIVES

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 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 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 CONTENT

Lesson 1: Identifying Security Fundamentals

- Identify Information Security Concepts
- Identify Basic Security Controls
- Identify Basic Authentication and Authorization Concepts
- Identify Basic Cryptography Concepts

Lesson 2: Analyzing Risk

- Analyze Organizational Risk
- Analyze the Business Impact of Risk

Lesson 3: Identifying Security Threats

- Identify Types of Attackers
- Identify Social Engineering Attacks
- Identify Malware
- Identify Software-Based Threats
- Identify Network-Based Threats
- Identify Wireless Threats
- Identify Physical Threats

Lesson 4: Conducting Security Assessments

- Identify Vulnerabilities
- Assess Vulnerabilities
- Implement Penetration Testing

Lesson 5: Implementing Host and Software Security

- Implement Host Security
- Implement Cloud and Virtualization Security
- Implement Mobile Device Security
- Incorporate Security in the Software Development Lifecycle

Lesson 6: Implementing Network Security

- Configure Network Security Technologies
- Secure Network Design Elements
- Implement Secure Networking Protocols and Services
- Secure Wireless Traffic

Lesson 7: Managing Identity and Access

- Implement Identity and Access Management
- Configure Directory Services
- Configure Access Services
- Manage Accounts

Lesson 8: Implementing Cryptography

- Identify Advanced Cryptography Concepts
- Select Cryptographic Algorithms
- Configure a Public Key Infrastructure
- Enroll Certificates
- Back Up and Restore Certificates and Private Keys
- Revoke Certificates

Lesson 9: Implementing Operational Security

- Evaluate Security Frameworks and Guidelines
- Incorporate Documentation in Operational Security
- Implement Security Strategies
- Manage Data Security Processes
- Implement Physical Controls

Lesson 10: Addressing Security Incidents

- Troubleshoot Common Security Issues
- Respond to Security Incidents
- Investigate Security Incidents

Lesson 11: Ensuring Business Continuity

- Select Business Continuity and Disaster Recovery Processes
- Develop a Business Continuity Plan