CompTIA® Security+® (Exam SY0-401)

Course Specifications

Course Length:

5 days

Course Description

Overview:

CompTIA® Security+® (Exam SY0-401) is the primary course 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 SY0-401) 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.

Course Objectives:

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

You will:

- Identify the fundamental concepts of computer security.
- Identify security threats and vulnerabilities.
- Manage data, application, and host security.
- Implement network security.
- Identify and implement access control and account management security measures.
- Manage certificates.
- Identify and implement compliance and operational security measures.
- Manage risk.
- Troubleshoot and manage security incidents.
- Plan for business continuity and disaster recovery.

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.

Prerequisites:

To ensure your success in your course, you should possess basic Windows user skills and a fundamental understanding of computer and networking concepts. You can obtain this level of skills and knowledge by taking one of the following LogicalCHOICE courses:

- *Using Microsoft® Windows® 8.1*
- *Microsoft® Windows® 8.1 Transition from Windows® 7*

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 LogicalCHOICE courses:

- *CompTIA® A+®: A Comprehensive Approach (Exams 220-801 and 220-802)*
- *CompTIA® Network+® (Exam N10-005)*

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. For instance, to gain experience with managing Windows Server® 2012, you could take any or all of the following LogicalCHOICE courses:

- *Microsoft® Windows® Server 2012: Installation and Configuration*
- *Microsoft® Windows® Server 2012: Administration*
- *Microsoft® Windows® Server 2012: Configuring Advanced Services*

Course Content

Lesson 1: Security Fundamentals

Topic A: The Information Security Cycle

Topic B: Information Security Controls

Topic C: Authentication Methods

Topic D: Cryptography Fundamentals

Topic E: Security Policy Fundamentals

Lesson 2: Identifying Security Threats and Vulnerabilities

Topic A: Social Engineering

Topic B: Malware

Topic C: Software-Based Threats

Topic D: Network-Based Threats

Topic E: Wireless Threats and Vulnerabilities

Topic F: Physical Threats and Vulnerabilities

Lesson 3: Managing Data, Application, and Host Security

Topic A: Manage Data Security

Topic B: Manage Application Security

Topic C: Manage Device and Host Security

Topic D: Manage Mobile Security

Lesson 4: Implementing Network Security

Topic A: Configure Security Parameters on Network Devices and Technologies

Topic B: Network Design Elements and Components

Topic C: Implement Networking Protocols and Services

Topic D: Apply Secure Network Administration Principles

Topic E: Secure Wireless Traffic

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

Topic A: Access Control and Authentication Services

Topic B: Implement Account Management Security Controls

Lesson 6: Managing Certificates

Topic A: Install a CA Hierarchy

Topic B: Enroll Certificates

Topic C: Secure Network Traffic by Using Certificates

Topic D: Renew Certificates

Topic E: Back Up and Restore Certificates and Private Keys

Topic F: Revoke Certificates

Lesson 7: Implementing Compliance and Operational Security

Topic A: Physical Security

Topic B: Legal Compliance

Topic C: Security Awareness and Training

Topic D: Integrate Systems and Data with Third Parties

Lesson 8: Risk Management

Topic A: Risk Analysis

Topic B: Implement Vulnerability Assessment Tools and Techniques

Topic C: Scan for Vulnerabilities

Topic D: Mitigation and Deterrent Techniques

Lesson 9: Troubleshooting and Managing Security Incidents

Topic A: Respond to Security Incidents

Topic B: Recover from a Security Incident

Lesson 10: Business Continuity and Disaster Recovery Planning

Topic A: Business Continuity

Topic B: Plan for Disaster Recovery

Topic C: Execute DRPs and Procedures