CompTIA Certification

SEC+501: CompTIA Security+

Learn the fundamental principles of planning and configuring business, computer and network security systems in this 5-day course. Practice your skills in a hands-on, online virtualized Windows server environment. Multiple client and server machines will be used to install, apply, harden, scan, configure, customize, and explore standard security settings and tools. Labs are designed to provide direct real-world experience and you get access for 6 months to practice your skills!

$2,795.00

- 5 Days
- Includes 6 month access to online labs

Upcoming Dates

Course Description

CompTIA Security+ certification validates knowledge of security fundamentals, basic risk identification and analysis, threat identification and assessment, IT infrastructure security, cryptography, operational security, and general security processes including incident response and business continuity.

Certification Track:

This course will prepare students to take the SY0-501 CompTIA Security+ Certification exam, for the objectives released in 2017 and first tested in October 2017.

CompTIA Security+ Certification has been created as a benchmark for entry-level security skills.

Completion of the CompTIA Security+ certification meets criteria for the DoD 8570.01-M Information Assurance Workforce Improvement Program requirements, as modified and enforced starting January 24, 2012. CompTIA Security+ training is becoming a mandate for persons seeking to enter or maintain a career where security implementation and leadership are pre-requisites.

Course Outline

Module 1 - Security Fundamentals

- Security Terms and Concepts
- Security Controls
- Authentication and Authorization Concepts
- Basic Cryptography concepts.

Module 2 – Analyzing Risk

- Organizational Risk
- Risk Possibilities

- Risk Impacts
- Risk Response
- Risk management

Module 3 – Identify Security Threats

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

Module 4 – Conducting Security Assessments

- Identify Vulnerabilities
- Assess Vulnerabilities
- Implement Penetration Testing

Module 5 – Host and Software Security

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

Module 6 – Network Security

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

Module 7 – Managing Identify and Access

- Identity and Access Management
- Directory Services (LDAP and Active Directory)
- Access Services \
- Managing Accounts

Module 8 – Implementing Cryptography

- Advanced Cryptography Concepts
- Cryptographic Algorithms
- Public Key Infrastructure
- Enroll Certificates
- Backup and Restore Certificates and Private Keys

- Revoke Certificates

Module 9 – Implementing Operational Security

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

Module 10 – Addressing Security Incidents

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

Module 11 – Ensuring Business Incidents

- Select Business Continuity
- Disaster Recover Processes
- Develop a Business Continuity Plan

Audience

This course is intended for students wishing to qualify for CompTIA Security+ certification. The qualification is aimed at computer and networking professionals with a minimum of 24 months experience. Since security is vital to all levels and job roles within an organization, it will also benefit PC support analysts, application developers, and senior managers in accounting, sales, product development, and marketing who need an introduction to security terms, concepts, and best practices even if certification is not the intended goal.

Prerequisites

Ideally, students should have successfully completed CompTIA A+ or Network+ certification and have around 24 months' experience of personal computer or networking support. Regardless of whether students have passed CompTIA A+ or Network+, it is recommended that they have the following skills and knowledge before starting this course in order to take full advantage of the materials:

- Know the function and basic features and components of a PC.
- Use Windows administrative tools (Explorer, Settings, Control Panel and Management Consoles) to create and manage files and basic features of the operating system.
- Basic network terminology (such as OSI Model, Topology, Ethernet, TCP/IP); TCP/IP addressing, core protocols, and troubleshooting tools.
- Basic use of desktop virtual workstation environments.

Our instructors guide students from basic introductions toward mastery of classroom topics. Course delivery supplements the following outline utilizing real world examples, class discussion, and provision of additional resources in support of student needs and/or inquiry.

What You Will Learn

On course completion, students will be able to:

- Identify device, network, and social attack strategies and defenses.

- Understand the principles of organizational security and the elements of effective security policies.
- Know the technologies and uses of encryption standards and products.
- Identify host-based, mobile, and centralized security technologies and practices.
- Describe how local and remote access security are enforced.
- Describe the standards and products used to investigate and enforce security on network and Internet enabled technologies.
- Identify strategies for ensuring business continuity, fault tolerance, and disaster recovery