

## Course Description

CompTIA Security+ validates knowledge of systems security, network infrastructure, access control, assessments and audits, cryptography and organizational security.

BTS works with clients to deliver appropriate material to become CompTIA Security+ certified. Course design uses the latest texts and other materials over a one or two week period based on client needs. The two week design includes extensive hands-on with security labs and security configurations. Time is allowed after each Instructor presentation and demonstration for student hands-on work on actual equipment, labs, practice exams and Security+ related drills. Students take the exam soon after class to become Security+ Certified. Based on the class design, customized slide presentations, and a tailored approach to class needs, student pass rates are often 100

The CompTIA Security+ certification designates knowledgeable professionals in the field of security, one of the fastest-growing fields in IT. Security threats are increasing in number and severity, and the gap between the need for security professionals and qualified IT personnel is the largest of any IT specialty, according to a 2008 CompTIA study. Even in a troubled economy, most businesses plan to maintain or increase their investment in security. CompTIA Security+ is an international, vendor-neutral certification that proves competency in system security, network infrastructure, access control and organizational security. Major organizations that employ CompTIA Security+ certified staff include Booz Allen Hamilton, Hewlett-Packard, IBM, Motorola, Symantec, Telstra, Hitachi, Ricoh, Lockheed Martin, Unisys, Hilton Hotels Corp., General Mills, the U.S. Navy, Army, Air Force and Marines. Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years of technical networking experience, with an emphasis on security. The CompTIA Network+ certification is also recommended.

For IT professionals requiring re-certification

The newest version of the CompTIA Security+ certification exam, SY0-201, was launched in

late 2008. IT professionals who are encouraged or required by their employers to remain current on their certifications have two options They can take the new version of the exam, or they can take the CompTIA Security+ bridge exam, which covers the new objectives. The test, exam code BR0-001, is a 60-minute, 50-question test available in English. A passing score is 560 on a scale of 100-900. Only professionals who are currently CompTIA Security+ certified under 2002 exam objectives are eligible to become CompTIA Security+ 2008 certified by taking the bridge exam

## Students Will Learn

- Basics of authentication and authorization
- Types of attacks and malicious code
- Remote access security
- Email and web security
- Wireless security
- Security design and security baselines
- Security monitoring and intrusion detection
- Physical security
- Security forensics

## Target Audience

This course is targeted toward an Information Technology (IT) professional who has networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems and to those who want to further a career in IT by acquiring a foundational knowledge of security topics prepare for the CompTIA Security+ Certification examination or use Security+ as the foundation for advanced security certifications.

## Prerequisites

CompTIA A+ and Network+ certifications, or equivalent knowledge. Experience in networking, including experience configuring and managing TCP/IP is beneficial.

## Course Outline

### Module I: Systems Security

- Differentiate among various systems security threats.
- Explain the security risks pertaining to system hardware and peripherals.
- Implement OS hardening practices and procedures to achieve workstation and server security.
- Carry out the appropriate procedures to establish application security.
- Implement security applications.
- Explain the purpose and application of virtualization technology.

### Module II: Network Infrastructure

- Differentiate between the different ports & protocols, their respective threats and mitigation techniques.
- Distinguish between network design elements and components.
- Determine the appropriate use of network security tools to facilitate network security.
- Apply the appropriate network tools to facilitate network security.
- Explain the vulnerabilities and mitigations associated with network devices.
- Explain the vulnerabilities and mitigations associated with various transmission media.
- Explain the vulnerabilities and implement mitigations associated with wireless networking.

### Module III: Access Control

- Identify and apply industry best practices for access control methods.
- Explain common access control models and the differences between each.
- Organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges.
- Apply appropriate security controls to file and print resources.
- Compare and implement logical access control methods.
- Summarize the various authentication models and identify the components of each.
- Deploy various authentication models and identify the components of each.
- Explain the difference between identification and authentication (identity proofing).
- Explain and apply physical access security methods.

#### Module IV: Assessments & Audits

- Conduct risk assessments and implement risk mitigation.
- Carry out vulnerability assessments using common tools.
- Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning.
- Use monitoring tools on systems and networks and detect security-related anomalies.
- Compare and contrast various types of monitoring methodologies.
- Execute proper logging procedures and evaluate the results.
- Conduct periodic audits of system security settings.

#### Module V: Cryptography

- Explain general cryptography concepts.
- Explain basic hashing concepts and map various algorithms to appropriate applications.
- Explain basic encryption concepts and map various algorithms to appropriate applications.
- Explain and implement protocols.
- Explain core concepts of public key cryptography.
- Implement PKI and certificate management.

#### Module VI: Organizational Security

- Explain redundancy planning and its components.
- Implement disaster recovery procedures.
- Differentiate between and execute appropriate incident response procedures.
- Identify and explain applicable legislation and organizational policies.
- Explain the importance of environmental controls.
- Explain the concept of and how to reduce the risks of social engineering.

## Delivery Method

Instructor led with numerous Hands-On labs and exercises.

## Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

## Course Length

5 Days