

# CompTIA Security+® (2008 Objectives)

**Course length: 5.0 day(s)**

## Course Description

CompTIA Security+® (2008 Objectives) is the primary course you will need to take if your job responsibilities include securing network services, network devices, and network traffic. It is also the main course you will take to prepare for the CompTIA Security+ (2008 Edition) Certification examination (exam number SY0-201). In this course, you will build on your knowledge and professional experience with computer hardware, operating systems, and networks as you acquire the specific skills required to implement basic security services on any type of computer network.

**Course Objective:** You will implement and monitor security on networks, applications, and operating systems, and respond to security breaches.

**Target Student:** 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, such as OS X, Unix, or Linux, and who wants 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 or career roles.

**Prerequisites:** Basic Windows skills and fundamental understanding of computer and networking concepts are required. CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP, are strongly recommended. Students can obtain this level of skill and knowledge by taking any of the following Element K courses: CompTIA A+ Certification and Network+ Certification. 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.

**Delivery Method:** Instructor led, group-paced, classroom-delivery learning model with structured hands-on activities.

## Performance-Based Objectives

Upon successful completion of this course, students will be able to:

- identify fundamental concepts of computer security.
- identify security threats.
- harden internal systems and services.
- harden internetwork devices and services.
- secure network communications.
- establish security best practices for creating and running web-based applications.
- manage public key infrastructure (PKI).
- manage certificates.
- enforce organizational security policies.
- monitor the security infrastructure.
- manage security incidents.

## Course Content

### Lesson 1: Security Fundamentals

Security Building Blocks

Authentication Methods

Cryptography Fundamentals

Security Policy Fundamentals

## **Lesson 2: Security Threats**

- Social Engineering
- Software-Based Threats
- Network-Based Threats
- Hardware-Based Threats

## **Lesson 3: Hardening Internal Systems and Services**

- Harden Operating Systems
- Harden Directory Services
- Harden DHCP Servers
- Harden File and Print Servers

## **Lesson 4: Hardening Internetwork Devices and Services**

- Harden Internetwork Connection Devices
- Harden DNS and BIND Servers
- Harden Web Servers
- Harden Email Servers
- Harden Conferencing and Messaging Servers
- Secure File Transfers

## **Lesson 5: Securing Network Communications**

- Protect Network Traffic with IP Security (IPSec)
- Secure Wireless Traffic
- Secure the Network Telephony Infrastructure
- Secure the Remote Access Channel

## **Lesson 6: Securing Web Applications**

- Prevent Input Validation Attacks
- Protect Systems from Buffer Overflow Attacks
- Implement ActiveX and Java Security
- Protect Systems from Scripting Attacks
- Implement Secure Cookies
- Harden a Web Browser

## **Lesson 7: Managing Public Key Infrastructure (PKI)**

- Install a Certificate Authority (CA) Hierarchy
- Harden a Certificate Authority
- Back Up a CA
- Restore a CA

## **Lesson 8: Managing Certificates**

- Enroll Certificates
- Secure Network Traffic by Using Certificates
- Renew Certificates
- Revoke Certificates
- Back Up Certificates and Private Keys
- Restore Certificates and Private Keys

## **Lesson 9: Enforcing Organizational Security Policies**

- Perform a Risk Assessment
- Enforce Corporate Security Policy Compliance
- Enforce Legal Compliance
- Enforce Physical Security Compliance
- Educate Users
- Plan for Disaster Recovery
- Conduct a Security Audit

## **Lesson 10: Monitoring the Security Infrastructure**

Scan for Vulnerabilities

Monitor for Security Anomalies

Set Up a Honeypot

## **Lesson 11: Managing Security Incidents**

Respond to Security Incidents

Evidence Administration

Recover From a Security Incident

## **Appendix A: Mapping Security+ Course Content to the CompTIA Security+ Exam Objectives**

## **Appendix B: CompTIA Security+ Acronyms**