

# CompTIA Security+ (2008 Objectives)

Course length: 5 days

## 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. Students can obtain this level of skill and knowledge by taking the following courses: Introduction to Networks and the Internet and any one or more of the following: Introduction to Personal Computers: Using Windows XP, Windows XP: Introduction, Introduction to Personal Computers: Using Windows Vista, Microsoft Windows Vista: Level 1 and Level 2. 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 courses: CompTIA A+ Certification: A Comprehensive Approach for all 2006 Exam Objectives, Network+ Certification: Fourth Edition – A CompTIA Certification or CompTIA Network+® (2009 Objectives)

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

- Topic 1A: Security Building Blocks
- Topic 1B: Authentication Methods
- Topic 1C: Cryptography Fundamentals
- Topic 1D: Security Policy Fundamentals

#### Lesson 2: Security Threats

- Topic 2A: Social Engineering
- Topic 2B: Software-Based Threats
- Topic 2C: Network-Based Threats
- Topic 2D: Hardware-Based Threats

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

- Topic 3A: Harden Operating Systems
- Topic 3B: Harden Directory Services
- Topic 3C: Harden DHCP Servers
- Topic 3D: Harden File and Print Servers

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

- Topic 4A: Harden Internetwork Connection Devices
- Topic 4B: Harden DNS and BIND Servers
- Topic 4C: Harden Web Servers
- Topic 4D: Harden Email Servers
- Topic 4E: Harden Conferencing and Messaging Servers
- Topic 4F: Secure File Transfers

#### Lesson 5: Securing Network Communications

- Topic 5A: Protect Network Traffic with IP Security (IPSec)
- Topic 5B: Secure Wireless Traffic
- Topic 5C: Secure the Network Telephony Infrastructure
- Topic 5D: Secure the Remote Access Channel

#### Lesson 6: Securing Web Applications

- Topic 6A: Prevent Input Validation Attacks
- Topic 6B: Protect Systems from Buffer Overflow Attacks
- Topic 6C: Implement ActiveX and Java Security
- Topic 6D: Protect Systems from Scripting Attacks
- Topic 6E: Implement Secure Cookies
- Topic 6F: Harden a Web Browser

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

- Topic 7A: Install a Certificate Authority (CA) Hierarchy
- Topic 7B: Harden a Certificate Authority
- Topic 7C: Back Up a CA
- Topic 7D: Restore a CA

#### Lesson 8: Managing Certificates

- Topic 8A: Enroll Certificates
- Topic 8B: Secure Network Traffic by Using Certificates



Topic 8C: Renew Certificates  
Topic 8D: Revoke Certificates  
Topic 8E: Back Up Certificates and Private Keys  
Topic 8F: Restore Certificates and Private Keys

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

Topic 9A: Perform a Risk Assessment  
Topic 9B: Enforce Corporate Security Policy Compliance  
Topic 9C: Enforce Legal Compliance  
Topic 9D: Enforce Physical Security Compliance  
Topic 9E: Educate Users  
Topic 9F: Plan for Disaster Recovery  
Topic 9G: Conduct a Security Audit

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

Topic 10A: Scan for Vulnerabilities  
Topic 10B: Monitor for Security Anomalies  
Topic 10C: Set Up a Honeypot

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

Topic 11A: Respond to Security Incidents  
Topic 11B: Evidence Administration  
Topic 11C: Recover From a Security Incident

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

**Appendix B:** CompTIA Security+ Acronyms

