



Number of Days: 5

Format: Instructor-Led

Recommended Course Sequence

Knowledge of prerequisites
noted below.

*Course content is subject to change
without notice.*

Security + Certification

Course Description:

The CompTIA Security+ certification tests for security knowledge mastery of an individual with two years on-the-job networking experience, with emphasis on security. The exam covers industry-wide topics, including communication security, infrastructure security, cryptography, access control, authentication, external attack and operational and organization security. CompTIA Security+ is taught at colleges, universities, and commercial training centers around the globe. There are approximately 13,000 CompTIA Security+ certified professionals worldwide. CompTIA Security+ is an elective or prerequisite to advanced security certifications. The objectives of CompTIA Security+ were derived through input from industry, government and academia, a job task analysis, a survey of more than 1,100 subject matter experts and a beta exam with responses from subject matter experts around the world.

Target Student:

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 NetWare, Macintosh, UNIX/Linux, and OS/2, 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:

CompTIA, A+ and Network+ certifications, or equivalent knowledge, and 6-9 months experience in networking, including experience configuring and managing TCP/IP, although not required, students might find it helpful to obtain foundational information from introductory operating system administration courses.

Delivery Method:

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

At Course Completion:

You will implement and monitor security on networks and computer systems, and respond to security breaches.

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

- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Manage a PKI.
- Manage certificates.
- Enforce an organizational security policy.
- Monitor the security infrastructure.

Security + Certification

Course Outline

Lesson 1: Identifying Security Threats
<ul style="list-style-type: none">■ Topic 1A: Identify Social Engineering Attacks■ Topic 1B: Classify Network Attacks■ Topic 1C: Classify Software-Based Attacks
Lesson 2: Hardening Internal Systems and Services
<ul style="list-style-type: none">■ Topic 2A: Harden Base Operating Systems■ Topic 2B: Harden Directory Services■ Topic 2C: Harden DHCP Servers■ Topic 2D: Harden Network File and Print Servers
Lesson 3: Hardening Internetwork Devices and Services
<ul style="list-style-type: none">■ Topic 3A: Harden Internetwork Connection Devices■ Topic 3B: Harden DNS and BIND Servers■ Topic 3C: Harden Web Servers■ Topic 3D: Harden FTP Servers■ Topic 3E: Harden Network News Transport Protocol (NNTP) Servers■ Topic 3F: Harden Email Servers■ Topic 3G: Harden Conferencing
Lesson 4: Lesson 4: Securing Network Communications
<ul style="list-style-type: none">■ Topic 4A: Secure Network Traffic Using IP Security (IPSec)■ Topic 4B: Secure Wireless Traffic■ Topic 4C: Secure Client Internet Access■ Topic 4D: Secure the Remote Access Channel
Lesson 5: Managing Public Key Infrastructure (PKI)
<ul style="list-style-type: none">■ Topic 5A: Install a Certificate Authority (CA) Hierarchy■ Topic 5B: Harden a Certificate Authority■ Topic 5C: Back Up Certificate Authorities■ Topic 5D: Restore a Certificate Authority
Lesson 6: Managing Certificates
<ul style="list-style-type: none">■ Topic 6A: Enroll Certificates for Entities■ Topic 6B: Secure Network Traffic Using Certificates■ Topic 6C: Renew Certificates■ Topic 6D: Revoke Certificates■ Topic 6E: Back Up Certificates and Private Keys■ Topic 6F: Restore Certificates and Private Keys
Lesson 7: Enforcing Organizational Security Policy
<ul style="list-style-type: none">■ Topic 7A: Enforce Corporate Security Policy Compliance■ Topic 7B: Enforce Legal Compliance■ Topic 7C: Enforce Physical Security Compliance■ Topic 7D: Educate Users
Lesson 8: Monitoring the Security Infrastructure
<ul style="list-style-type: none">■ Topic 8A: Scan for Vulnerabilities■ Topic 8B: Monitor for Intruders■ Topic 8C: Set Up a Honey pot■ Topic 8D: Respond to Security Incidents