

Course Description: Security+™ A CompTIA Certification 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+ examination (exam number SY0-101). In this course, you'll 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.

Who Should Attend: 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 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: Students should have CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine 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.

Benefits of Attendance: Upon 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.

Course Outline:

Identifying Security Threats

Identify Social Engineering Attacks
Classify Software Attacks
Identify Hardware Attacks

Hardening Internal Systems and Services

Harden Base Operating Systems
Harden Directory Services
Harden DHCP Servers
Harden Network File and Print Servers

Hardening Internetwork Devices and Services

Harden Internetwork Connection Devices
Harden DNS and BIND Servers
Harden Web Servers
Harden FTP Servers
Harden Network News Transport Protocol (NNTP) Servers
Harden Email Servers
Harden Conferencing and Messaging Servers

Securing Network Communications

Secure Network Traffic Using IP Security (IPSec)
Secure Wireless Traffic
Secure Client Internet Access
Secure the Remote Access Channel

Managing Public Key Infrastructure (PKI)

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

Managing Certificates

Enroll Certificates for Entities
Secure Network Traffic Using Certificates
Renew Certificates
Revoke Certificates
Back Up Certificates and Private Keys
Restore Certificates and Private Keys

Enforcing Organizational Security Policy

Enforce Corporate Security Policy Compliance
Enforce Legal Compliance
Enforce Physical Security Compliance
Educate Users

Monitoring the Security Infrastructure

Scan for Vulnerabilities
Monitor for Intruders
Set Up a Honeypot
Respond to Security Incidents