



Security+™: A CompTIA Certification

Course length: 5.0 day(s)

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.

Course Objective: You will implement and monitor security on networks and computer 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 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 six to nine months experience in networking, including experience configuring and managing TCP/IP. Students can obtain this level of skill and knowledge by taking the following Element K courses: A+ Certification: Core Hardware A+ Certification: Operating Systems Network+ Certification: 3rd Edition

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 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.



Course Content

Lesson 1: Identifying Security Threats

- Topic 1A: Identify Social Engineering Attacks
- Topic 1B: Classify Software Attacks
- Topic 1C: Identify Hardware Attacks

Lesson 2: Hardening Internal Systems and Services

- 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

- 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 and Messaging Servers

Lesson 4: Securing Network Communications

- 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)

- 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

- 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

- 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

- Topic 8A: Scan for Vulnerabilities
- Topic 8B: Monitor for Intruders
- Topic 8C: Set Up a Honeypot
- Topic 8D: Respond to Security Incidents

Appendix A: Authentication and Authorization

Appendix B: Understanding Media Supplemental Lesson

- Topic 1A: Removable Media
- Topic 1B: Cabling

Appendix C: SecureSystems.doc

Appendix D: Security+ Exam Objectives Mapping

Appendix E: Automated Setup Instructions