

# CompTIA Security+

## 5 Day Course

Locations: Mex, D.F.

Date:

## 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 CompTIA A+ and Network+ courses, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP, are strongly recommended.



## Table of Contents

### 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

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

### 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

