

COURSE	TITLE	DURATION
CompTIA	Security+ Certification	40 H.

**Overview:**

This course focuses on providing the skills and knowledge necessary to prepare students for the CompTIA Security+ Certification Exam. This course provides the broad-based knowledge necessary to prepare for further study in specialized security fields.

**At Course Completion:**

Upon successful completion of this course, students will be able to: - To identify fundamental concepts of computer security and security threats - The skills to harden internal systems and services as well as internetwork devices and service - How to implement secure network communications - To establish security best practices for creating and running web-based applications. - How to manage public key infrastructure (PKI) and certificates. - How to enforce organizational security policies. - The necessities to monitor the security infrastructure and manage security incidents.

**Prerequisites:**

There are no enforced prerequisites, however the recommended prerequisites are the CompTIA Network+ certification and two years of technical networking experience with an emphasis on security.

**Course Outlines:**

**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

### **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