

CompTIA: Security+ Course Summary

Description

CompTIA Security+® (2008 Objectives) 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+ (2008 Edition) Certification examination (exam number SY0-201). In this course, you will 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.

Objectives

At the end of this course, students will be able to:

- Identify fundamental concepts of computer security.
- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Establish security best practices for creating and running web-based applications.
- Manage public key infrastructure (PKI).
- Manage certificates.
- Enforce organizational security policies.
- Monitor the security infrastructure.
- Manage security incidents.

Topics

- Security Fundamentals
- Security Threats
- Hardening Internal Systems and Services
- Hardening Internetwork Devices and Services
- Securing Network Communications
- Securing Web Applications
- Managing Public Key Infrastructure (PKI)
- Managing Certificates
- Enforcing Organizational Security Policies
- Monitoring the Security Infrastructure
- Managing Security Incidents
- Appendix A: Mapping Security+ Course Content to the CompTIA Security+ Exam Objectives
- Appendix B: CompTIA Security+ Acronyms

Audience

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 following courses: Introduction to Networks and the Internet and any one or more of the following: Introduction to Personal Computers: Using Windows XP, Introduction to Personal Computers: Using Windows Vista, Microsoft Windows Vista: Level 1 and Level 2, CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP, are strongly recommended. Students can obtain this level of skill and knowledge by taking any of the following courses: CompTIA A+ Certification: A Comprehensive Approach for all 2006 Exam Objectives, Network+ Certification: Fourth Edition – A CompTIA Certification or CompTIA Network+® (2009 Objectives)

Additional introductory courses or work experience in application development and programming or in network and operating system administration for any software platform or system are helpful but not required.

Duration

Five days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically.

CompTIA: Security+

Course Outline

I. Security Fundamentals

- A. Security Building Blocks: Authentication Methods
- B. Cryptography Fundamentals
- C. Security Policy Fundamentals

II. Security Threats

- A. Social Engineering
- B. Software-Based Threats
- C. Network-Based Threats
- D. Hardware-Based Threats

III. Hardening Internal Systems and Services

- A. Harden Operating Systems
- B. Harden Directory Services
- C. Harden DHCP Servers
- D. Harden File and Print Servers

IV. Hardening Internetwork Devices and Services

- A. Harden Internetwork Connection Devices
- B. Harden DNS and BIND Servers
- C. Harden Web Servers
- D. Harden Email Servers
- E. Harden Conferencing and Messaging Servers
- F. Secure File Transfers

V. Securing Network Communications

- A. Protect Network Traffic with IP Security (IPSec)
- B. Secure Wireless Traffic
- C. Secure the Network Telephony Infrastructure
- D. Secure the Remote Access Channel

VI. Securing Web Applications

- A. Prevent Input Validation Attacks
- B. Protect Systems from Buffer Overflow Attacks
- C. Implement ActiveX and Java Security
- D. Protect Systems from Scripting Attacks
- E. Implement Secure Cookies
- F. Harden a Web Browser

VII. Managing Public Key Infrastructure (PKI)

- A. Install a Certificate Authority (CA) Hierarchy
- B. Harden a Certificate Authority
- C. Back Up a CA
- D. Restore a CA

VIII. Managing Certificates

- A. Enroll Certificates
- B. Secure Network Traffic by Using Certificates
- C. Renew Certificates
- D. Revoke Certificates
- E. Back Up Certificates and Private Keys
- F. Restore Certificates and Private Keys

IX. Enforcing Organizational Security Policies

- A. Perform a Risk Assessment
- B. Enforce Corporate Security Policy Compliance
- C. Enforce Legal Compliance
- D. Enforce Physical Security Compliance
- E. Educate Users
- F. Plan for Disaster Recovery
- G. Conduct a Security Audit

X. Monitoring the Security Infrastructure

- A. Scan for Vulnerabilities
- B. Monitor for Security Anomalies
- C. Set Up a Honeytrap

XI. Managing Security Incidents

- A. Respond to Security Incidents
- B. Evidence Administration
- C. Recover From a Security Incident

XII. Appendix A: Mapping Security+ Course Content to the CompTIA Security+ Exam Objectives

XIII. Appendix B: CompTIA Security+ Acronyms