



DEEP CREEK CENTER

Delivering Results

SECURITY + CERTIFICATION (5 DAYS)

OVERVIEW

CompTIA Security+® 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.

COURSE OBJECTIVE

You will implement and monitor security on networks, applications, and operating 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 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.

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.

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.

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 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.

COURSE CONTENT

Lesson 1: Security Fundamentals

Topic 1A: Security Building Blocks

Topic 1B: Authentication Methods

Topic 1C: Cryptography Fundamentals

Topic 1D: Security Policy Fundamentals

Lesson 2: Security Threats

Topic 2A: Social Engineering

Topic 2B: Software-Based Threats

Topic 2C: Network-Based Threats

Topic 2D: Hardware-Based Threats

Lesson 3: Hardening Internal Systems and Services

Topic 3A: Harden Operating Systems

Topic 3B: Harden Directory Services

Topic 3C: Harden DHCP Servers

Topic 3D: Harden File and Print Servers

Lesson 4: Hardening Internetwork Devices and Services

Topic 4A: Harden Internetwork Connection Devices

Topic 4B: Harden DNS and BIND Servers

Topic 4C: Harden Web Servers

Topic 4D: Harden Email Servers

Topic 4E: Harden Conferencing and Messaging Servers

Topic 4F: Secure File Transfers

Lesson 5: Securing Network Communications

Topic 5A: Protect Network Traffic with IP Security (IPSec)

Topic 5B: Secure Wireless Traffic

Topic 5C: Secure the Network Telephony Infrastructure

Topic 5D: Secure the Remote Access Channel

Lesson 6: Securing Web Applications

Topic 6A: Prevent Input Validation Attacks

Topic 6B: Protect Systems from Buffer Overflow Attacks

Topic 6C: Implement ActiveX and Java Security

Topic 6D: Protect Systems from Scripting Attacks

Topic 6E: Implement Secure Cookies

Topic 6F: Harden a Web Browser

Lesson 7: Managing Public Key Infrastructure (PKI)

Topic 7A: Install a Certificate Authority (CA) Hierarchy

Topic 7B: Harden a Certificate Authority

Topic 7C: Back Up a CA

Topic 7D: Restore a CA

Lesson 8: Managing Certificates

Topic 8A: Enroll Certificates

Topic 8B: Secure Network Traffic by Using Certificates

Topic 8C: Renew Certificates

Topic 8D: Revoke Certificates

Topic 8E: Back Up Certificates and Private Keys

Topic 8F: Restore Certificates and Private Keys

Lesson 9: Enforcing Organizational Security Policies

Topic 9A: Perform a Risk Assessment

Topic 9B: Enforce Corporate Security Policy Compliance

Topic 9C: Enforce Legal Compliance

Topic 9D: Enforce Physical Security Compliance

Topic 9E: Educate Users

Topic 9F: Plan for Disaster Recovery

Topic 9G: Conduct a Security Audit

Lesson 10: Monitoring the Security Infrastructure

Topic 10A: Scan for Vulnerabilities

Topic 10B: Monitor for Security Anomalies

Topic 10C: Set Up a Honeypot

Lesson 11: Managing Security Incidents

Topic 11A: Respond to Security Incidents

Topic 11B: Evidence Administration

Topic 11C: Recover From a Security Incident