CompTIA Security+ Bootcamp

Length: 5 days
Format: Bootcamp
Time: Day

About This Course

CompTIA Security+ is the primary course you will need to take if your job responsibilities include securing network services, devices, and traffic in your organization. You can also take this course to prepare for the CompTIA Security+ certification examination. In this course, you will build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.

This primary goal of this course is to help each student pass the exams required to earn the Security+ certification. To do this, your knowledgeable instructor will blend hands-on labs with lecture and practice exams to prepare you to pass each exam. The practice exams identify knowledge gaps that the instructor will fill with customized, hands-on labs and tailored lectures. Our on-site testing center allows you to take the exam when you are ready.

Click here to find your place on the CompTIA Roadmap.

To learn more about the course objectives and opportunities in the industry for Security+ certified professionals, view our Security+ Certification Info Session.

Required Exams

SY0-501

Audience Profile

This course is targeted toward the information technology (IT) professional who has networking and administrative skills in Windows-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; familiarity with other operating systems, such as Mac OS, Unix, or Linux; and who wants to further a career in IT by acquiring 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.

Course Objectives

After completing this course, students will be able to:

* Identify the fundamental concepts of computer security.
* Identify security threats and vulnerabilities.
* Manage data, application, and host security.
* Implement network security.
* Identify and implement access control and account management security measures.
* Manage certificates.
* Identify and implement compliance and operational security measures.
* Manage risk.
* Troubleshoot and manage security incidents.
* Plan for business continuity and disaster recovery.

Outline

Section 1:Security Fundamentals * The Information Security Cycle
* Information Security Controls
* Authentication Methods
* Cryptography Fundamentals
* Security Policy Fundamentals

Section 2:Identifying Security Threats and Vulnerabilities * Social Engineering
* Malware
* Software-Based Threats
* Network-Based Threats
* Wireless Threats and Vulnerabilities
* Physical Threats and Vulnerabilities

Section 3:Managing Data, Application, and Host Security * Manage Data Security
* Manage Application Security
* Manage Device and Host Security
* Manage Mobile Security

Section 4:Implementing Network Security * Configure Security Parameters on Network Devices and Technologies
* Network Design Elements and Components
* Implement Networking Protocols and Services
* Apply Secure Network Administration Principles
* Secure Wireless Traffic

Section 5:Implementing Access Control, Authentication, and Account Management * Access Control and Authentication Services
* Implement Account Management Security Controls

Section 6:Managing Certificates * Install a CA Hierarchy
* Enroll Certificates
* Secure Network Traffic by Using Certificates
* Renew Certificates
* Back Up and Restore Certificates and Private Keys
* Revoke Certificates

Section 7:Implementing Compliance and Operational Security * Physical Security
* Legal Compliance
* Security Awareness and Training
* Integrate Systems and Data with Third Parties

Section 8:Risk Management * Risk Analysis
* Implement Vulnerability Assessment Tools and Techniques
* Scan for Vulnerabilities
* Mitigation and Deterrent Techniques

Section 9:Troubleshooting and Managing Security Incidents * Respond to Security Incidents
* Recover from a Security Incident

Section 10:Business Continuity and Disaster Recovery Planning * Business Continuity
* Plan for Disaster Recovery
* Execute DRPs and Procedures