



Official CompTIA Content
for Instructor-Led Training:

Security+ Student Guide 2019 UPDATE

Official CompTIA Content for Instructor-Led Training is designed with the instructor in mind, providing insights and tools on how to successfully train learners pursuing their CompTIA Security+ certification.

Overview

The Official CompTIA Security+ Guide 2019 UPDATE (Exam SY0-501) is developed exclusively by CompTIA, combining market-leading content with instructor input and the latest instructional design techniques. A refreshed organization of content, additional assessments, scenario-based exercises and exclusive video from ITPro.TV delivers an integrated solution for preparing students for the Security+ certification exam.

Official CompTIA Content:

- The Official CompTIA Security+ Instructor Guide 2019 UPDATE (Exam SY0-501)
- The Official CompTIA Security+ Student Guide 2019 UPDATE (Exam SY0-501)
- CompTIA CHOICE Digital Learning Platform
 - Online resources included with purchase of student or instructor guide
- The Official CompTIA Security+ LogicalLAB 2019 UPDATE (Exam SY0-501)
- CompTIA CertMaster Practice for Security+ (Exam SY0-501)

New Features in the 2019 UPDATE

- **Alignment and Consistency Across Book, Labs and Assessment:** With CompTIA developing all learning materials, the book, labs and assessments work together with a similar approach and voice ensuring that instructors and students have a cohesive “single-sourced” solution for their Security+ courses.
- **Reorganization lessons:** More lessons (16 compared 11 in the previous edition) distinguish more clearly between functional areas associated with information security roles. The content sequence has been revised, with early lessons providing hands-on activity opportunities with cybersecurity tools and software, before proceeding through identity and access management concepts. Lessons conclude with risk management, software development and security policy uses.
- **Comprehensive Activities:** Hands-on activities have been re-conceived as longer, more comprehensive, lab-style exercises. In addition, extensive review and discussion activities have been added.
- **Hands-on Practice with Virtual Labs:** LogicalLABS hosted by Learn on Demand Systems allows learning in actual software applications through a remote environment. The 2019 Update aligns with the refreshed lab activities. Students have 6 months of access, providing a fantastic resource for students to practice their skills.
- **Engaging Video Program by ITPro.TV:** New videos developed exclusively for CompTIA by ITPro.TV provide short, engaging demonstrations of key activities in the course. The videos provide an alternative to hands-on demonstrations.
- **Robust Assessments:** The Security+ 2019 Update provides practice questions for each lesson and a final assessment covering all lessons, more than 250 questions in total. Additionally, performance-based questions help students apply what they have learned in actual scenarios.
- **Refreshed Interior Design and Image Program:** A modernized interior design updates the presentation of content. More images have been added throughout to complement the narrative and provide visual interest.

Key Features and Benefits

- **Designed and class-tested Instructor-Led Training:** Topics are presented in a hierarchy delivering knowledge, procedural tasks and hand-on activities, keeping students engaged.
- **Comprehensive student and instructor resources enhanced through CompTIA CHOICE platform:**
Resources to download include:
 - Course setup notes describe hardware and software requirements
 - Course-specific delivery tips with in-sights to deliver the course material
 - Presentation planners help schedule courses based on the length
 - PowerPoint slides
 - Facilitator notes in instructor manual
 - Solutions to activities and discussions
 - Video program with ITPro.TV
- **100% coverage of job-role focused exam objectives:** Content is practical, based on real performance scenarios. In addition, content is aligned to certification exam objectives.
- **Flexible and customizable based on course format:** Class resources can be easily configured based on modality.

Lab Options

- Labs can be delivered in the classroom with the help of course setup notes, or LogicalLABS allow students to learn in through a remote lab environment. Lab activities are available for each lesson.

Exam Prep Option

- CertMaster Practice is an online assessment and remediation tool designed to help students feel more confident and prepared for their CompTIA certification exam.

Course Overview



This course is for students who are preparing to take the CompTIA Security+ certification exam SY0-501.

This course is aimed toward the IT professional who has networking and administrative skills in Windows-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; plus familiarity with other operating systems, such as macOS, Unix or Linux; and who wants to further a career in IT by acquiring foundational knowledge of security topics.

Job Roles

- Systems Administrator
- Security Administrator
- Security Specialist
- Security Engineer
- Network Administrator
- Junior IT Auditor/Penetration Tester
- Security Consultant

Updated Resources

Labs Available:

- ACTIVITY 1-5: Exploring the Lab Environment
- ACTIVITY 1-6: Determining Malware Types
- ACTIVITY 3-3: Performing Network Scanning with Software Tools
- ACTIVITY 3-5: Analyzing Network Traffic with Packet Sniffing Software Tools
- ACTIVITY 3-6: Concealing Data with Steganography Tools
- ACTIVITY 3-8: Identifying Vulnerabilities with Scanning Software Tools
- ACTIVITY 4-4: Implementing Certificate Services
- ACTIVITY 5-3: Deploying Certificates and Implementing Key Recovery
- ACTIVITY 6-3: Cracking Passwords using Software Tools
- ACTIVITY 7-5: Managing Accounts in a Windows Domain
- ACTIVITY 8-5: Implementing a Secure Network Design
- ACTIVITY 9-3: Installing and Configuring a Firewall
- ACTIVITY 9-5: Installing and Configuring an Intrusion Detection System
- ACTIVITY 12-2: Implementing Secure Network Addressing Services
- ACTIVITY 12-4: Implementing a Virtual Private Network
- ACTIVITY 13-3: Installing and Configuring a Secure Email Service
- ACTIVITY 14-6: Using Forensic Tools
- ACTIVITY 15-2: Identifying a Man-in-the-Browser Attack

Performance-based Questions Available:

- Lesson 1: Comparing and Contrasting Attacks
- Lesson 5: Implementing Public Key Infrastructure
- Lesson 9: Installing and Configuring Security Appliances
- Lesson 13: Implementing Secure Network Applications
- Lesson 15: Summarizing Secure Application Development Concepts

Prerequisites

Students should have basic Windows user skills and a fundamental understanding of computer and networking concepts. Achievement of CompTIA A+ and Network+ certifications, plus two years of experience with IT administration with a security focus.

Course content summary

Lesson 1: Comparing and Contrasting Attacks

Topic 1A: Compare and Contrast Information Security Roles
Topic 1B: Explain Threat Actor Types
Topic 1C: Compare and Contrast Social Engineering Attack Types
Topic 1D: Determine Malware Types

Lesson 2: Comparing and Contrasting Security Controls

Topic 2A: Compare and Contrast Security Control and Framework Types
Topic 2B: Follow Incident Response Procedures

Lesson 3: Using Security Assessment Tools

Topic 3A: Explain Penetration Testing Concepts
Topic 3B: Use Topology Discovery Software Tools
Topic 3C: Use Fingerprinting and Sniffing Software Tools
Topic 3D: Use Vulnerability Scanning Software Tools

Lesson 4: Comparing and Contrasting Basic Concepts of Cryptography

Topic 4A: Compare and Contrast Basic Concepts of Cryptography
Topic 4B: Compare and Contrast Cryptographic Attack Types
Topic 4C: Explain Hashing and Symmetric Cryptographic Algorithms
Topic 4D: Explain Asymmetric Cryptographic Algorithms

Lesson 5: Implementing Public Key Infrastructure

Topic 5A: Implement Certificates and Certificate Authorities
Topic 5B: Implement PKI Management
Lesson 6: Implementing Identity and Access Management Controls
Topic 6A: Compare and Contrast Identity and Authentication Concepts
Topic 6B: Install and Configure Authentication Protocols
Topic 6C: Implement Multifactor Authentication

Lesson 7: Managing Access Services and Accounts

Topic 7A: Install and Configure Authorization and Directory Services
Topic 7B: Implement Access Management Controls
Topic 7C: Differentiate Account Management Practices
Topic 7D: Implement Account Auditing and Recertification

Lesson 8: Implementing Secure Network Architecture Concepts

Topic 8A: Implement Secure Network Architecture Concepts
Topic 8B: Install and Configure Secure Switching Infrastructure
Topic 8C: Install and Configure Network Access Control
Topic 8D: Install and Configure Secure Routing and NAT Infrastructure

Lesson 9: Installing and Configuring Security Appliances

Topic 9A: Install and Configure Firewalls and Proxies
Topic 9B: Install and Configure Load Balancers
Topic 9C: Install and Configure Intrusion Detection/Prevention Systems
Topic 9D: Install and Configure Logging and SIEM Systems

Lesson 10: Installing and Configuring Wireless and Physical Access Security

Topic 10A: Install and Configure Wireless Infrastructure
Topic 10B: Install and Configure Wireless Security Settings
Topic 10C: Explain the Importance of Physical Security Controls

Lesson 11: Deploying Secure Host, Embedded, and Mobile Systems

Topic 11A: Implement Secure Hardware Systems Design
Topic 11B: Implement Secure Host Systems Design
Topic 11C: Implement Secure Embedded Systems Design
Topic 11D: Implement Secure Mobile Device Systems Design

Lesson 12: Implementing Secure Network Access Protocols

Topic 12A: Implement Secure Network Operations Protocols
Topic 12B: Implement Secure Remote Access Protocols
Topic 12C: Implement Secure Remote Administration Protocols

Lesson 13: Implementing Secure Network Applications

Topic 13A: Implement Secure Web Services
Topic 13B: Implement Secure Communications Services
Topic 13C: Implement Secure Virtualization Infrastructure
Topic 13D: Implement Secure Cloud Services

Lesson 14: Explaining Risk Management and Disaster Recovery Concepts

Topic 14A: Explain Risk Management Processes and Concepts
Topic 14B: Explain Disaster Recovery Planning Concepts
Topic 14C: Explain Resiliency and Continuity of Operations Strategies
Topic 14D: Summarize Basic Concepts of Forensics

Lesson 15: Summarizing Secure Application Development Concepts

Topic 15A: Explain the Impact of Vulnerability Types
Topic 15B: Summarize Secure Application Development Concepts

Lesson 16: Explaining Organizational Security Concepts

Topic 16A: Explain the Importance of Security Policies
Topic 16B: Implement Data Security and Privacy Practices
Topic 16C: Explain the Importance of Personnel Management

Appendix A: Mapping Course Content to CompTIA Security+ (Exam SY0-501)
Solutions (Student Guide only, solutions are included "in line" in the Instructor Guide)
Glossary
Index



Purchase Everything in One Place

Official CompTIA Content is available on the CompTIA Store at store.comptia.org, which means partners will be able to obtain Official CompTIA Content, CompTIA CertMaster products and exam vouchers all in one place.

Please contact your CompTIA business development representative for more information.

