

Soft-Train



*At Soft-Train
Technology Works*

CompTIA Security+

(5 Days)
ST32006

COURSE GOAL: To prepare for the CompTIA Security+ Certification Exam SY0-301

PREREQUISITES: Basic understanding of computer operations. CompTIA A+ and Network+ certification highly recommended.

LEARNING OBJECTIVES:

Upon completion of this course the student will be able to:

- Identify general security concepts
- Understand security issues with remote access, email and web components
- Understand infrastructure security issues
- Utilize cryptography techniques
- Understand operational security techniques
- Employ administrative controls

KEY TOPICS:

I. Measuring and Weighing Risk

- A. Risk Assessment
- B. Computing Risk
- C. Developing Policies, Standards, and Guidelines
- D. Implementing Policies
- E. Incorporating Standards

II. Infrastructure and Connectivity

- A. Mastering TCP/IP
- B. Distinguishing Between Security Topologies
- C. Understanding Infrastructure Security
- D. Working with Hardware Components
- E. Understanding Remote Access

III. Protecting Networks

- A. Monitoring and Diagnosing Networks
- B. Understanding Intrusion Detection Systems
- C. Understanding Protocol Analyzers
- D. Securing Workstations and Servers
- E. Securing Internet Connections
- F. Understanding Network Protocols

IV. Threats and Vulnerabilities

- A. Understanding Software Exploitation
- B. Surviving Malicious Code
- C. Calculating Attack Strategies
- D. Recognizing Common Attacks
- E. Identifying TCP/IP Security Concerns

V. Access Control and Identity Management

- A. Access Control Basics
- B. Understanding Remote Access Connectivity
- C. Understanding Authentication Services
- D. Understanding Access Control
- E. Implementing Access Control Best Practices

VI. Educating and Protecting the User

- A. Understanding Security Awareness and Training
- B. Classifying Information
- C. Information Access Controls
- D. Complying with Privacy and Security Regulations
- E. Understanding Social Engineering

VII. Operating System and Application Security

- A. Hardening the Operating System
- B. Application Hardening
- C. Working with Data Repositories
- D. Host Security

E. Mobile Devices

VIII. Cryptography Basics

- A. An Overview of Cryptography
- B. Understanding Cryptographic Algorithms
- C. Using Cryptographic Systems
- D. Understanding Cryptography Standards and Protocols

IX. Cryptography Implementation

- A. Using Public Key Infrastructure
- B. Preparing for Cryptographic Attacks
- C. Understanding Key management and the Key Life Cycle
- D. Recovering and Archiving Keys

X. Physical and Hardware-Based Security

- A. Implementing Access Control
- B. Maintaining Environmental and Power Controls
- C. EMI Shielding
- D. Fire Suppression

XI. Security and Vulnerability in the Network

- A. Network Security Threats
- B. Secure Network Administration Principles
- C. Mitigation and Deterrent Techniques
- D. Monitoring System Logs

- XII. Wireless Networking Security**
 - A. Working with Wireless Systems
 - B. Wireless Transport Layer Security
 - C. Understanding Mobile Devices
 - D. Wireless Vulnerabilities to Know

- XIII. Disaster Recovery and Incident Response**
 - A. Understanding Business Continuity
 - B. Undertaking Business Impact Analysis
 - C. Utilities
 - D. High Availability
 - E. Disaster Recovery
 - F. Incident Response Policies

- XIV. Security-Related Policies and Procedures**
 - A. Policies You Must Have
 - B. Policies You Should Have
 - C. Certificate Policies
 - D. Security Controls for Account Management

- XV. Security Administration**
 - A. Security Administrator's Troubleshooting Guide
 - B. Creating a Home Lab
 - C. Access Control Issues
 - D. Auditing
 - E. Authentication Schemes
 - F. File sharing Basics
 - G. Working with IDSs and Honey Pots
 - H. Incident Handling

- I. Internet Common Sense
- J. Key Management Conventions
- K. Preventing Common Malicious Events
- L. Managing Personnel
- M. Keeping Physical Security Meaningful
- N. Securing the Infrastructure Working with Security Zones
- O. Social Engineering Risk
- P. System Hardening Basics
- Q. Securing the Wireless Environment