CompTIA Security+ Day

Length: 9 days
Format: Classroom
Time: Day

About This Course

CompTIA Security+ validates knowledge of systems security, network infrastructure, access control, assessments and audits, cryptography and organizational security. It is an international, vendor-neutral security certification that is taught at colleges, universities and commercial training centers around the world.

Because human error is the number one cause for a network security breach, CompTIA Security+ is recognized by the technology community as a valuable credential that proves competency with information security. Many corporations recommend or require the Security+ certification for their IT employees. Network security is a major issue for corporations today and as the demand for secure networks grows, Security+ is quickly becoming the standard. CompTIA Security+ is the perfect addition to any networking career.

Click here to find your place on the CompTIA pathway.

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

Required Exams

Audience Profile

This course is intendend for students who want to acquire a solid foundation in computer security and whoâ€™s goal is to prepare for the CompTIA Security+ exam by learning how to develop and improve security. Itâ€™s designed for students who want to acquire hands-on skills and in-depth knowledge of computer security.

Course Objectives

After completing this course, students will be able to:

* Identify and help mitigate security risksâ€”essential concepts
* Know and apply the basic principles of cryptography, keys, and certificates
* Monitor and help secure vulnerabilities in TCP/IP and network infrastructure

* Help protect e-mail, RAS, VPNs, wireless services, and other online communications
* Configure user and group privileges, access control, and authentication
* Implement security baselines, system updates, and intrusion detection
* Create an operational security planâ€”from physical security to business continuity
* Build an organizational security programâ€”documentation, risk assessment

Outline

Module 1 - Measuring and Weighing Risk * Risk Assessment * Computing Risk Assessment
* Acting on Your Risk Assessment
* Risks Associated with Cloud Computing
* Risks Associated with Virtualization

* Developing Policies, Standards, and Guidelines * Implementing Policies
* Incorporating Standards
* Following Guidelines
* Business Policies
* Understanding Control Types, False Positives, and Change and Incident Management

Module 2 - Infrastructure and Connectivity * Mastering TCP/IP 9 * Working with the TCP/IP Suite
* IPv4 vs. IPv6
* Understanding Encapsulation
* Working with Protocols and Services

* Distinguishing between Security Topologies * Setting Design Goals
* Creating Security Zones
* Working with Newer Technologies
* Working with Business Requirements

* Understanding Infrastructure Security * Working with Hardware Components
* Working with Software Components

* Understanding the Different Network Infrastructure Devices * Firewalls
* Hubs

* Modems
* Remote Access Services
* Routers
* Switches
* Load Balancers
* Telecom/PBX Systems
* Virtual Private Networks
* Web Security Gateway
* Spam Filters

* Understanding Remote Access * Using Point-to-Point Protocol
* Working with Tunneling Protocols

Module 3 - Protecting Networks * Monitoring and Diagnosing Networks * Network Monitors
* Intrusion Detection Systems

* Understanding Intrusion Detection Systems * Working with a Network-Based IDS
* Working with a Host-Based IDS
* Working with NIPS
* Utilizing Honeypots

* Understanding Protocol Analyzers
* Securing Workstations and Servers
* Securing Internet Connections * Working with Ports and Sockets
* Working with Email
* Working with the Web
* Working with File Transfer Protocol

* Understanding Network Protocols

Module 4 - Threats and Vulnerabilities * Understanding Software Exploitation
* Surviving Malicious Code * Viruses
* Trojan Horses
* ContentsÂ xv
* Logic Bombs
* Worms

* Antivirus Software

* Calculating Attack Strategies * Understanding Access Attack Types
* Recognizing Modification and Repudiation Attacks
* Identifying Denial-of-Service and DistributedÂ Denial-of-Service Attacks
* Recognizing Botnets

* Recognizing Common Attacks * Backdoor Attacks
* Spoofing Attacks
* Pharming Attacks
* Phishing and Spear Phishing Attacks
* Man-in-the-Middle Attacks
* Replay Attacks
* Password-Guessing Attacks
* Privilege Escalation

* Identifying TCP/IP Security Concerns * Recognizing TCP/IP Attacks

Module 5 - Access Control and Identity Management * Access Control Basics * Identification vs. Authentication
* Authentication (Single Factor) and Authorization
* Multifactor Authentication
* Operational Security
* Tokens
* Potential Authentication and Access Problems
* Authentication Issues to Consider

* Understanding Remote Access Connectivity * Using the Point-to-Point Protocol
* Working with Tunneling Protocols
* Working with RADIUS
* TACACS/TACACS+/XTACACS
* VLAN Management

* Understanding Authentication Services * LDAP
* Kerberos

* Single Sign-On Initiatives

* Understanding Access Control * Mandatory Access Control
* Discretionary Access Control
* Role-Based Access Control
* Rule-Based Access Control

* Implementing Access Control Best Practices * Smart Cards
* Access Control Lists
* Trusted OS
* Secure Router Configuration

Module 6 - Educating and Protecting the User * Understanding Security Awareness and Training * Communicating with Users to Raise Awareness
* Providing Education and Training
* Training Topics

* Classifying Information * Public Information
* Private Information

* Information Access Controls
* Complying with Privacy and Security Regulations * The Health Insurance Portability and
* Accountability Act
* The Gramm-Leach-Bliley Act
* The Computer Fraud and Abuse Act
* The Family Educational Rights and Privacy Act
* The Computer Security Act of 1987
* The Cyberspace Electronic Security Act
* The Cyber Security Enhancement Act
* The Patriot Act
* Familiarizing Yourself with International Efforts

* Understanding Social Engineering * Types of Social Engineering Attacks
* What Motivates an Attack?
* Social Engineering Attack Examples

Module 7 - Operating System and Application Security * Hardening the Operating System * The Basics of OS Hardening
* Hardening Filesystems
* Updating Your Operating System

* Application Hardening * Fuzzing
* Cross-Site Request Forgery
* Application Configuration Baselining
* Application Patch Management
* Making Your Network More Secure Through Hardening

* Working with Data Repositories * Directory Services
* Databases and Technologies
* Injection Problems
* SQL Injection
* LDAP Injection
* XML Injection
* Directory Traversal/Command Injection

* Host Security * Antimalware
* Host Software Baselining

* Mobile Devices
* Best Practices for Security * URL Filtering
* Content Inspection
* Malware Inspection
* Data Loss Prevention
* Data Encryption
* Hardware-Based Encryption Devices

* Attack Types to Be Aware Of * Session Hijacking
* Header Manipulation

Module 8 - Cryptography Basics * An Overview of Cryptography * Understanding Non-mathematical Cryptography
* Understanding Mathematical Cryptography
* Working with Passwords
* Understanding Quantum Cryptography
* Uncovering the Myth of Unbreakable Codes

* Understanding Cryptographic Algorithms * The Science of Hashing
* Working with Symmetric Algorithms
* Working with Asymmetric Algorithms
* Wi-Fi Encryption

* Using Cryptographic Systems * Confidentiality
* Integrity
* Digital Signatures
* Authentication
* Non-repudiation
* Access Control
* Key Features

* Understanding Cryptography Standards and Protocols * The Origins of Encryption Standards
* Public-Key Infrastructure X.509/Public-Key Cryptography Standards
* X.509
* SSL and TLS
* Certificate Management Protocols
* Secure Multipurpose Internet Mail Extensions
* Secure Electronic Transaction
* Secure Shell
* Pretty Good Privacy
* HTTP Secure
* Secure HTTP
* IP Security
* Tunneling Protocols
* Federal Information Processing Standard

Module 9 - Cryptography Implementation * Using Public Key Infrastructure * Using a Certificate Authority

* Working with Registration Authorities and Local Registration Authorities
* Implementing Certificates
* Understanding Certificate Revocation
* Implementing Trust Models

* Preparing for Cryptographic Attacks * Ways to Attack Cryptographic Systems
* Three Types of Cryptographic Attacks

* Understanding Key Management and the Key Life Cycle * Methods for Key Generation
* Storing and Distributing Keys
* Using Key Escrow
* Identifying Key Expiration
* Revoking Keys
* Suspending Keys
* Recovering and Archiving Keys
* Renewing Keys
* Destroying Keys
* Identifying Key Usage

Module 10 - Physical and Hardware-Based Security * Implementing Access Control * Physical Barriers
* Security Zones
* Partitioning
* Biometrics

* Maintaining Environmental and PowerÂ Controls * Environmental Monitoring
* Power Systems
* EMI Shielding
* Hot and Cold Aisles

* Fire Suppression * Fire Extinguishers
* Fixed Systems

Module 11 - Security and Vulnerability in theÂ Network * Network Security Threats * Penetration Testing

* Vulnerability Scanning
* Ethical Hacking
* Assessment Types and Techniques

* Secure Network Administration Principles * Rule-Based Management
* Port Security
* Working with 802.1X
* Flood Guards and Loop Protection
* Preventing Network Bridging
* Log Analysis

* Mitigation and Deterrent Techniques * Manual Bypassing of Electronic Controls
* Monitoring System Logs
* Security Posture
* Reporting
* Detection/Prevention Controls

Module 12 - Wireless Networking Security * Working with Wireless Systems * IEEE 802.11 x Wireless Protocols
* WEP/WAP/WPA/WPA2
* Wireless Transport Layer Security

* Understanding Mobile Devices * Wireless Access Points
* Extensible Authentication Protocol
* Lightweight Extensible Authentication Protocol
* Protected Extensible Authentication Protocol

* Wireless Vulnerabilities to Know

Module 13 - Disaster Recovery and Incident Response * Understanding Business Continuity * Undertaking Business Impact Analysis
* Utilities
* High Availability
* Disaster Recovery
* Incident Response Policies
* Understanding Incident Response

* Succession Planning

* Reinforcing Vendor Support * Service-Level Agreements
* Code Escrow Agreements

Module 14 - Security-Related Policies and Procedures * Policies You Must Have * Data Loss/Theft Policies
* Least Privilege
* Separation of Duties
* Time of Day Restrictions
* Mandatory Vacations and Job Rotation

* Policies You Should Have * Human Resource Policies
* Certificate Policies

* Security Controls for Account Management * User and Group Role Management
* Users with Multiple Accounts/Roles
* Auditing
* Account Policy Enforcement

Module 15 - Security Administration * Security Administratorâ€™s Troubleshooting Guide
* Getting Started * Creating a Home Lab
* In the Workplace
* Which OS Should You Use?
* Creating a Security Solution

* Access Control Issues
* Accountability Concerns
* Auditing
* Authentication Schemes * Authentication Factors
* Mutual Authentication
* Authentication Protection

* Backup Management
* Baselining Security
* Certificate Management
* Communications Security * Preauthentication
* Remote Control/Remote Shell
* Virtual Private Networks

* Directory Services Protection
* Disaster Planning
* Documenting Your Environment
* Email Issues
* File-Sharing Basics
* Working with IDSs and Honey Pots
* Incident Handling
* Internet Common Sense
* Key Management Conventions
* Preventing Common Malicious Events * Constructing a Line of Defense
* Types of Attacks
* Antivirus Protection
* Making Stronger Passwords

* Managing Personnel
* Keeping Physical Security Meaningful
* Securing the Infrastructure
* Working with Security Zones
* Social Engineering Risks
* System Hardening Basics
* Securing the Wireless Environment