Security+
Exam SY0-501

Overview
The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. The successful candidate will perform these tasks to support the principles of confidentiality, integrity, and availability.

Course Length
5 days

Target Student
CompTIA Security+ is aimed at IT professionals with job roles such as security architect, security engineer, security consultant/ specialist, information assurance technician, security administrator, systems administrator, and network administrator.

Ideally, you should have successfully completes the " CompTIA Network+ Support Skills" course and have around 24 months experience of networking support or IT administration. It is not necessary that you pass the Network + exam before completing Security+ certification, but it is recommended.

Regardless of whether you have passed Network+, it is recommended that you have the following skills and knowledge before starting this course:

- Know the function and basic features of the components of a PC
- Use Windows Server to create and manage files and use basic administrative features (Explores, Control Panel, Management Consoles)
- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, TCP/IP, switches, routers)
- Understand TCP/IP addressing, core protocols, and troubleshooting tools.

Prerequisites
- CompTIA Network+ and two years of experience in IT administration with a security focus

Course Objectives

This course will teach you the fundamentals principles of identifying risk and implementing security controls. I t will prepare you to take the CompTIA Security+ exam providing 100% coverage of the objectives and content examples listed on the syllabus. On course completion, you will be able to:

- Identify network attack strategies and defenses
- Understand the principles of organizational security and the elements of effective security policies
- Identify network- and host- based security technologies and practices
- Describe how wireless and remote access security is enforced
- Describe the standards and products used to enforce security on web and communications technologies
- Identify strategies for ensuring business continuity, fault tolerance, and disaster recovery.

Course Contents

- Threats, Attacks and Vulnerabilities
  - Given a scenario, analyze indicators of compromise and determine the type of malware.

    Viruses
    - Crypto-malware
    - Ransomware
    - Worm
    - Trojan
    - Rootkit
    - Keylogger
    - Adware
    - Spyware
    - Bots
    - RAT
    - Logic bomb
    - Backdoor
  - Compare and contrast types of attacks.
    - Social engineering
    - Application/service attacks

- Wireless attacks
- Cryptographic attacks

- Explain threat actor types and attributes.
  - Types of actors
  - Attributes of actors
  - Use of open-source intelligence
- Explain penetration testing concepts.
  - Active reconnaissance
  - Passive reconnaissance
  - Pivot
  - Initial exploitation
  - Persistence
  - Escalation of privilege
  - Black box
  - White box
  - Gray box
  - Pen testing vs. vulnerability scanning
- Explain vulnerability scanning concepts.
  - Passively test security controls
  - Identify vulnerability
  - Identify lack of security controls
  - Identify common misconfigurations
  - Intrusive vs. non-intrusive
  - Credentialed vs. non-credentialed
  - False positive
- Explain the impact associated with types of vulnerabilities.
  - Race conditions
  - Vulnerabilities due to:
  - Improper input handling
  - Improper error handling
  - Misconfiguration/weak configuration
  - Default configuration

- Resource exhaustion
- Untrained users
- Improperly configured accounts
- Vulnerable business processes
- Weak cipher suites and implementations
- Memory/buffer vulnerability
- System sprawl/undocumented assets
- Architecture/design weaknesses
- New threats/zero day
- Improper certificate and key management

- Technologies and Tools
  - Install and configure network components, both hardware- and software-based, to support organizational security.
    - Firewall
    - VPN concentrator
    - NIPS/NIDS
    - Router
    - Switch
    - Proxy
    - Load balancer
    - Access point
    - SIEM
    - DLP
    - NAC
    - Mail gateway
    - Bridge
    - SSL/TLS accelerators
    - SSL decryptors
    - Media gateway
    - Hardware security module
  - Given a scenario, use appropriate software tools to assess the security posture of an organization.
    - Protocol analyzer

- Network scanners
- Wireless scanners/cracker
- Password cracker
- Vulnerability scanner
- Configuration compliance scanner
- Exploitation frameworks
- Data sanitization tools
- Steganography tools
- Honeypot
- Backup utilities
- Banner grabbing
- Passive vs. active
- Command line tools

- Given a scenario, troubleshoot common security issues.
  - Unencrypted credentials/clear text
  - Logs and events anomalies
  - Permission issues
  - Access violations
  - Certificate issues
  - Data exfiltration
  - Misconfigured devices
  - Weak security configurations
  - Personnel issues
  - Unauthorized software
  - Baseline deviation
  - License compliance violation (availability/integrity)
  - Asset management
  - Authentication issues
- Given a scenario, analyze and interpret output from security technologies.
  - HIDS/HIPS
  - Antivirus
  - File integrity check
  - Host-based firewall

- Application whitelisting
- Removable media control
- Advanced malware tools
- Patch management tools
- UTM
- DLP
- Data execution prevention
- Web application firewall

- Given a scenario, deploy mobile devices securely.
  - Connection methods
  - Mobile device management concepts
  - Enforcement and monitoring for:
  - Deployment models
- Given a scenario, implement secure protocols.
  - Protocols
  - Use cases

- Architecture and Design
  - Explain use cases and purpose for frameworks, best practices and secure configuration guides.
    - Industry-standard frameworks and reference architectures
    - Benchmarks/secure configuration guides
    - Defense-in-depth/layered security
  - Given a scenario, implement secure network architecture concepts.
    - Zones/topologies
    - Segregation/segmentation/isolation
    - Tunneling/VPN
    - Security device/technology placement
    - SDN
  - Given a scenario, implement secure systems design.
    - Hardware/firmware security
    - Operating systems
    - Peripherals
  - Explain the importance of secure staging deployment concepts.

- Sandboxing
- Environment
- Secure baseline
- Integrity measurement

- Explain the security implications of embedded systems.
  - SCADA/ICS
  - Smart devices/IoT
  - HVAC
  - SoC
  - RTOS
  - Printers/MFDs
  - Camera systems
  - Special purpose
- Summarize secure application development and deployment concepts.
  - Development life-cycle models
  - Secure DevOps
  - Version control and change management
  - Provisioning and deprovisioning
  - Secure coding techniques
  - Code quality and testing
  - Compiled vs. runtime code
- Summarize cloud and virtualization concepts.
  - Hypervisor
  - VM sprawl avoidance
  - VM escape protection
  - Cloud storage
  - Cloud deployment models
  - On-premise vs. hosted vs. cloud
  - VDI/VDE
  - Cloud access security broker
  - Security as a Service
- Explain how resiliency and automation strategies reduce risk.
  - Automation/scripting

- Templates
- Master image
- Non-persistence
- Elasticity
- Scalability
- Distributive allocation
- Redundancy
- Fault tolerance
- High availability
- RAID

- Explain the importance of physical security controls.
  - Lighting
  - Signs
  - Fencing/gate/cage
  - Security guards
  - Alarms
  - Safe
  - Secure cabinets/enclosures
  - Protected distribution/Protected cabling
  - Airgap
  - Mantrap
  - Faraday cage
  - Lock types
  - Biometrics
  - Barricades/bollards
  - Tokens/cards
  - Environmental controls
  - Cable locks
  - Screen filters
  - Cameras
  - Motion detection
  - Logs
  - Infrared detection

- Key management

- Identity and Access Management
  - Compare and contrast identity and access management concepts.
    - Identification, authentication, authorization and accounting (AAA)
    - Multifactor authentication
    - Federation
    - Single sign-on
    - Transitive trust
  - Given a scenario, install and configure identity and access services.
    - LDAP
    - Kerberos
    - TACACS+
    - CHAP
    - PAP
    - MSCHAP
    - RADIUS
    - SAML
    - OpenID Connect
    - OAUTH
    - Shibboleth
    - Secure token
    - NTLM
  - Given a scenario, implement identity and access management controls.
    - Access control models
    - Physical access control
    - Biometric factors
    - Tokens
    - Certificate-based authentication
    - File system security
    - Database security
  - Given a scenario, differentiate common account management practices.
    - Account types
    - General Concepts

- Account policy enforcement

- Risk Management
  - Explain the importance of policies, plans and procedures related to organizational security.
    - Standard operating procedure
    - Agreement types
    - Personnel management
    - General security policies
  - Summarize business impact analysis concepts.
    - RTO/RPO
    - MTBF
    - MTTR
    - Mission-essential functions
    - Identification of critical systems
    - Single point of failure
    - Impact
    - Privacy impact assessment
    - Privacy threshold assessment
  - Explain risk management processes and concepts.
    - Threat assessment
    - Risk assessment
    - Change management
  - Given a scenario, follow incident response procedures.
    - Incident response plan
    - Incident response process
  - Summarize basic concepts of forensics.
    - Order of volatility
    - Chain of custody
    - Legal hold
    - Data acquisition
    - Preservation
    - Recovery

- Strategic intelligence/counterintelligence gathering
- Track man-hours

- Explain disaster recovery and continuity of operation concepts.
  - Recovery sites
  - Order of restoration
  - Backup concepts
  - Geographic considerations
  - Continuity of operation planning
- Compare and contrast various types of controls.
  - Deterrent
  - Preventive
  - Detective
  - Corrective
  - Compensating
  - Technical
  - Administrative
  - Physical
- Given a scenario, carry out data security and privacy practices.
  - Data destruction and media sanitization
  - Data sensitivity labeling and handling
  - Data roles
  - Data retention
  - Legal and compliance

- Cryptography and PKI
  - Compare and contrast basic concepts of cryptography.
    - Symmetric algorithms
    - Modes of operation
    - Asymmetric algorithms
    - Hashing
    - Salt, IV, nonce
    - Elliptic curve
    - Weak/deprecated algorithms
    - Key exchange

- Digital signatures
- Diffusion
- Confusion
- Collision
- Steganography
- Obfuscation
- Stream vs. block
- Key strength
- Session keys
- Ephemeral key
- Secret algorithm
- Data-in-transit
- Data-at-rest
- Data-in-use
- Random/pseudo-random number generation
- Key stretching
- Implementation vs. algorithm selection
- Perfect forward secrecy
- Security through obscurity
- Common use cases

- Explain cryptography algorithms and their basic characteristics.
  - Symmetric algorithms
  - Cipher modes
  - Asymmetric algorithms
  - Hashing algorithms
  - Key stretching algorithms
  - Obfuscation
- Given a scenario, install and configure wireless security settings.
  - Cryptographic protocols
  - Authentication protocols
  - Methods
- Given a scenario, implement public key infrastructure.
  - Components

- Concepts
- Types of certificates
- Certificate formats

Certification Information

- Exam SY0-501