Certification Exam Objectives: SY0-301

INTRODUCTION

The CompTIA Security+ Certification is a vendor neutral credential. The CompTIA Security+ exam is an internationally recognized validation of foundation-level security skills and knowledge, and is used by organizations and security professionals around the globe.

The CompTIA Security+ exam will certify that the successful candidate has the knowledge and skills required to identify risk and participate in risk mitigation activities, provide infrastructure, application, operational and information security, apply security controls to maintain confidentiality, integrity and availability, identify appropriate technologies and products, and operate with an awareness of applicable policies, laws and regulations.

The CompTIA Security+ Certification is aimed at an IT security professional who has:

- A minimum of 2 years experience in IT administration with a focus on security
- Day to day *technical* information security experience
- Broad knowledge of security concerns and implementation including the topics in the domain list below

CompTIA Security+ is ISO 17024 Accredited (Personnel Certification Accreditation) and, as such, undergoes regular reviews and updates to the exam objectives. The following CompTIA Security+ objectives reflect the subject areas in this edition of this exam, and result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an information security professional with two years of experience.

This examination blueprint includes domain weighting, test objectives, and example content. Example topics and concepts are included to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

The table below lists the domain areas measured by this examination and the approximate extent to which they are represented in the examination:

Domain	% of Examination
1.0 Network Security	21%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	21%
4.0 Application, Data and Host Security	16%
5.0 Access Control and Identity Management	13%
6.0 Cryptography	11%
Total	**100%**

**Note: The lists of examples provided in bulleted format below each objective are not exhaustive lists. Other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document.

1.0 Network Security

1.1 Explain the security function and purpose of network devices and technologies

- Firewalls
- Routers
- Switches
- Load Balancers
- Proxies
- Web security gateways
- VPN concentrators
- NIDS and NIPS (Behavior based, signature based, anomaly based, heuristic)
- Protocol analyzers
- Sniffers
- Spam filter, all-in-one security appliances
- Web application firewall vs. network firewall
- URL filtering, content inspection, malware inspection

1.2 Apply and implement secure network administration principles

- Rule-based management
- Firewall rules
- VLAN management
- Secure router configuration
- Access control lists
- Port Security
- 802.1x
- Flood guards
- Loop protection
- Implicit deny
- Prevent network bridging by network separation
- Log analysis

1.3 Distinguish and differentiate network design elements and compounds

- DMZ
- Subnetting
- VLAN
- NAT
- Remote Access
- Telephony
- NAC
- Virtualization
- Cloud Computing
    - Platform as a Service
    - Software as a Service
    - Infrastructure as a Service

1.4 Implement and use common protocols

- IPSec
- SNMP

- SSH
- DNS
- TLS
- SSL
- TCP/IP
- FTPS
- HTTPS
- SFTP
- SCP
- ICMP
- IPv4 vs. IPv6

1.5 Identify commonly used default network ports

- FTP
- SFTP
- FTPS
- TFTP
- TELNET
- HTTP
- HTTPS
- SCP
- SSH
- NetBIOS

1.6 Implement wireless network in a secure manner

- WPA
- WPA2
- WEP
- EAP
- PEAP
- LEAP
- MAC filter
- SSID broadcast
- TKIP
- CCMP
- Antenna Placement
- Power level controls

2.0 Compliance and Operational Security

2.1 Explain risk related concepts

- Control types
  - Technical
  - Management
  - Operational
- False positives
- Importance of policies in reducing risk
  - Privacy policy
  - Acceptable use
  - Security policy
  - Mandatory vacations

    - Job rotation
    - Separation of duties
    - Least privilege
- Risk calculation
    - Likelihood
    - ALE
    - Impact
- Quantitative vs. qualitative
- Risk-avoidance, transference, acceptance, mitigation, deterrence
- Risks associated to Cloud Computing and Virtualization

2.2 Carry out appropriate risk mitigation strategies

- Implement security controls based on risk
- Change management
- Incident management
- User rights and permissions reviews
- Perform routine audits
- Implement policies and procedures to prevent data loss or theft

2.3 Execute appropriate incident response procedures

- Basic forensic procedures
    - Order of volatility
    - Capture system image
    - Network traffic and logs
    - Capture video
    - Record time offset
    - Take hashes
    - Screenshots
    - Witnesses
    - Track man hours and expense
- Damage and loss control
- Chain of custody
- Incident response: first responder

2.4 Explain the importance of security related awareness and training

- Security policy training and procedures
- Personally identifiable information
- Information classification: Sensitivity of data (hard or soft)
- Data labeling, handling and disposal
- Compliance with laws, best practices and standards
- User habits
    - Password behaviors
    - Data handling
    - Clean desk policies
    - Prevent tailgating
    - Personally owned devices
- Threat awareness
    - New viruses
    - Phishing attacks
    - Zero days exploits
- Use of social networking and P2P

2.5 Compare and contrast aspects of business continuity

- Business impact analysis

- Removing single points of failure
- Business continuity planning and testing
- Continuity of operations
- Disaster recovery
- IT contingency planning
- Succession planning

2.6 Explain the impact and proper use of environmental controls

- HVAC
- Fire suppression
- EMI shielding
- Hot and cold aisles
- Environmental monitoring
- Temperature and humidity controls
- Video monitoring

2.7 Execute disaster recovery plans and procedures

- Backup / backout contingency plans or policies
- Backups, execution and frequency
- Redundancy and fault tolerance
    - Hardware
    - RAID
    - Clustering
    - Load balancing
    - Servers
- High availability
- Cold site, hot site, warm site
- Mean time to restore, mean time between failures, recovery time objectives and recovery point objectives

2.8 Exemplify the concepts of confidentiality, integrity and availability (CIA)

3.0 Threats and Vulnerabilities

3.1 Analyze and differentiate among types of malware

- Adware
- Virus
- Worms
- Spyware
- Trojan
- Rootkits
- Backdoors
- Logic bomb
- Botnets

3.2 Analyze and differentiate among types of attacks

- Man-in-the-middle
- DDoS
- DoS
- Replay
- Smurf attack

- Spoofing
- Spam
- Phishing
- Spim
- Vishing
- Spear phishing
- Xmas attack
- Pharming
- Privilege escalation
- Malicious insider threat
- DNS poisoning and ARP poisoning
- Transitive access
- Client-side attacks

3.3 Analyze and differentiate among types of social engineering attacks

- Shoulder surfing
- Dumpster diving
- Tailgating
- Impersonation
- Hoaxes
- Whaling
- Vishing

3.4 Analyze and differentiate among types of wireless attacks

- Rogue access points
- Interference
- Evil twin
- War driving
- Bluejacking
- Bluesnarfing
- War chalking
- IV attack
- Packet sniffing

3.5 Analyze and differentiate among types of application attacks

- Cross-site scripting
- SQL injection
- LDAP injection
- XML injection
- Directory traversal/command injection
- Buffer overflow
- Zero day
- Cookies and attachments
- Malicious add-ons
- Session hijacking
- Header manipulation

3.6 Analyze and differentiate among types of mitigation and deterrent techniques

- Manual bypassing of electronic controls
    - Failsafe/secure vs. failopen
- Monitoring system logs
    - Event logs
    - Audit logs

    - Security logs
    - Access logs
- Physical security
    - Hardware locks
    - Mantraps
    - Video surveillance
    - Fencing
    - Proximity readers
    - Access list
- Hardening
    - Disabling unnecessary services
    - Protecting management interfaces and applications
    - Password protection
    - Disabling unnecessary accounts
- Port security
    - MAC limiting and filtering
    - 802.1x
    - Disabling unused ports
- Security posture
    - Initial baseline configuration
    - Continuous security monitoring
    - remediation
- Reporting
    - Alarms
    - Alerts
    - Trends
- Detection controls vs. prevention controls
    - IDS vs. IPS
    - Camera vs. guard

3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities

- Vulnerability scanning and interpret results
- Tools
    - Protocol analyzer
    - Sniffer
    - Vulnerability scanner
    - Honeypots
    - Honeynets
    - Port scanner
- Risk calculations
    - Threat vs. likelihood
- Assessment types
    - Risk
    - Threat
    - Vulnerability
- Assessment technique
    - Baseline reporting
    - Code review
    - Determine attack surface
    - Architecture
    - Design reviews

3.8 Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning

- Penetration testing
    - Verify a threat exists
    - Bypass security controls
    - Actively test security controls
    - Exploiting vulnerabilities
- Vulnerability scanning
    - Passively testing security controls
    - Indentify vulnerability
    - Indentify lack of security controls
    - Indentify common misconfiguration
- Black box
- White box
- Gray box

4.0 Application, Data and Host Security

4.1 Explain the importance of application security

- Fuzzing
- Secure coding concepts
    - Error and exception handling
    - Input validation
- Cross-site scripting prevention
- Cross-site Request Forgery (XSRF) prevention
- Application configuration baseline (proper settings)
- Application hardening
- Application patch management

4.2 Carry out appropriate procedures to establish host security

- Operating system security and settings
- Anti-malware
    - Anti-virus
    - Anti-spam
    - Anti-spyware
    - Pop-up blockers
    - Host-based firewalls
- Patch management
- Hardware security
    - Cable locks
    - Safe
    - Locking cabinets
- Host software baselining
- Mobile devices
    - Screen lock
    - Strong password
    - Device encryption
    - Remote wipe/sanitation
    - Voice encryption
    - GPS tracking
- Virtualization

4.3 Explain the importance of data security

- Data Loss Prevention (DLP)
- Data encryption
  - Full disk
  - Database
  - Individual files
  - Removable media
  - Mobile devices
- Hardware based encryption devices
  - TPM
  - HSM
  - USB encryption
  - Hard drive
- Cloud computing

5.0 Access Control and Identity Management

5.1 Explain the function and purpose of authentication services

- RADIUS
- TACACS
- TACACS+
- Kerberos
- LDAP
- XTACACS

5.2 Explain the fundamental concepts and best practices related to authentication, authorization and access control

- Identification vs. authentication
- Authentication (single factor) and authorization
- Multifactor authentication
- Biometrics
- Tokens
- Common access card
- Personal identification verification card
- Smart card
- Least privilege
- Separation of duties
- Single sign on
- ACLs
- Access control
- Mandatory access control
- Discretionary access control
- Role/rule-based access control
- Implicit deny
- Time of day restrictions
- Trusted OS
- Mandatory vacations
- Job rotation

5.3 Implement appropriate security controls when performing account management

- Mitigates issues associated with users with multiple account/roles
- Account policy enforcement

    - Password complexity
    - Expiration
    - Recovery
    - Length
    - Disablement
    - Lockout
- Group based privileges
- User assigned privileges

6.0 Cryptography

6.1 Summarize general cryptography concepts

- Symmetric vs. asymmetric
- Fundamental differences and encryption methods
    - Block vs. stream
- Transport encryption
- Non-repudiation
- Hashing
- Key escrow
- Steganography
- Digital signatures
- Use of proven technologies
- Elliptic curve and quantum cryptography

6.2 Use and apply appropriate cryptographic tools and products

- WEP vs. WPA/WPA2 and preshared key
- MD5
- SHA
- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA
- RC4
- One-time-pads
- CHAP
- PAP
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- Whole disk encryption
- TwoFish
- Comparative strengths of algorithms
- Use of algorithms with transport encryption
    - SSL
    - TLS
    - IPSec
    - SSH
    - HTTPS

6.3 Explain the core concepts of public key infrastructure

- Certificate authorities and digital certificates
  - CA
  - CRLs
- PKI
- Recovery agent
- Public key
- Private key
- Registration
- Key escrow
- Trust models

6.4 Implement PKI, certificate management and associated components

- Certificate authorities and digital certificates
  - CA
  - CRLs
- PKI
- Recovery agent
- Public key
- Private keys
- Registration
- Key escrow
- Trust models

SECURITY+ ACRONYMS

3DES – Triple Digital Encryption Standard
AAA – Authentication, Authorization, and Accounting
ACL – Access Control List
AES - Advanced Encryption Standard
AES256 – Advanced Encryption Standards 256bit
AH - Authentication Header
ALE - Annualized Loss Expectancy
AP - Access Point
ARO - Annualized Rate of Occurrence
ARP - Address Resolution Protocol
AUP - Acceptable Use Policy
BCP – Business Continuity Planning
BIOS – Basic Input / Output System
BOTS – Network Robots
CA – Certificate Authority
CAC - Common Access Card
CAN - Controller Area Network
CCMP – Counter-Mode/CBC-Mac Protocol
CCTV - Closed-circuit television
CERT – Computer Emergency Response Team
CHAP – Challenge Handshake Authentication Protocol
CIRT – Computer Incident Response Team
CRC – Cyclical Redundancy Check
CRL – Certification Revocation List
DAC – Discretionary Access Control
DDOS – Distributed Denial of Service
DEP – Data Execution Prevention
DES – Digital Encryption Standard
DHCP – Dynamic Host Configuration Protocol
DLL - Dynamic Link Library
DLP - Data Loss Prevention
DMZ – Demilitarized Zone
DNS – Domain Name Service (Server)
DOS – Denial of Service
DRP – Disaster Recovery Plan
DSA – Digital Signature Algorithm
EAP - Extensible Authentication Protocol
ECC - Elliptic Curve Cryptography
EFS – Encrypted File System
EMI – Electromagnetic Interference

ESP – Encapsulated Security Payload
FTP – File Transfer Protocol
GPU - Graphic Processing Unit
GRE - Generic Routing Encapsulation
HDD – Hard Disk Drive
HIDS – Host Based Intrusion Detection System
HIPS – Host Based Intrusion Prevention System
HMAC – Hashed Message Authentication Code
HSM – Hardware Security Module
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol over SSL
HVAC – Heating, Ventilation Air Conditioning
IaaS - Infrastructure as a Service
ICMP - Internet Control Message Protocol
ID – Identification
IKE – Internet Key Exchange
IM - Instant messaging
IMAP4 - Internet Message Access Protocol v4
IP - Internet Protocol
IPSEC – Internet Protocol Security
IRC - Internet Relay Chat
ISP – Internet Service Provider
IV - Initialization Vector
KDC - Key Distribution Center
L2TP – Layer 2 Tunneling Protocol
LANMAN – Local Area Network Manager
LDAP – Lightweight Directory Access Protocol
LEAP – Lightweight Extensible Authentication Protocol
MAC – Mandatory Access Control / Media Access Control
MAC - Message Authentication Code
MAN - Metropolitan Area Network
MBR – Master Boot Record
MD5 – Message Digest 5
MSCHAP – Microsoft Challenge Handshake Authentication Protocol
MTU - Maximum Transmission Unit
NAC – Network Access Control
NAT – Network Address Translation
NIDS – Network Based Intrusion Detection System
NIPS – Network Based Intrusion Prevention System
NIST – National Institute of Standards & Technology
NOS – Network Operating System
NTFS - New Technology File System

NTLM – New Technology LANMAN
NTP - Network Time Protocol
OS – Operating System
OVAL – Open Vulnerability Assessment Language
PAP – Password Authentication Protocol
PAT - Port Address Translation
PBX – Private Branch Exchange
PEAP – Protected Extensible Authentication Protocol
PED - Personal Electronic Device
PGP – Pretty Good Privacy
PII – Personally Identifiable Information
PKI – Public Key Infrastructure
POTS – Plain Old Telephone Service
PPP - Point-to-point Protocol
PPTP – Point to Point Tunneling Protocol
PSK – Pre-Shared Key
PTZ – Pan-Tilt-Zoom
RA – Recovery Agent
RAD - Rapid application development
RADIUS – Remote Authentication Dial-in User Server
RAID – Redundant Array of Inexpensive Disks
RAS – Remote Access Server
RBAC – Role Based Access Control
RBAC – Rule Based Access Control
RSA – Rivest, Shamir, & Adleman
RTO – Recovery Time Objective
RTP – Real-Time Transport Protocol
S/MIME – Secure / Multipurpose internet Mail Extensions
SaaS - Software as a Service
SCAP - Security Content Automation Protocol
SCSI - Small Computer System Interface
SDLC - Software Development Life Cycle
SDLM - Software Development Life Cycle Methodology
SHA – Secure Hashing Algorithm
SHTTP – Secure Hypertext Transfer Protocol
SIM – Subscriber Identity Module
SLA – Service Level Agreement
SLE - Single Loss Expectancy
SMS - Short Message Service
SMTP – Simple Mail Transfer Protocol
SNMP - Simple Network Management Protocol
SONET – Synchronous Optical Network Technologies

SPIM - Spam over Internet Messaging
SSH – Secure Shell
SSL – Secure Sockets Layer
SSO – Single Sign On
STP – Shielded Twisted Pair
TACACS – Terminal Access Controller Access Control System
TCP/IP – Transmission Control Protocol / Internet Protocol
TKIP - Temporal Key Integrity Protocol
TLS – Transport Layer Security
TPM – Trusted Platform Module
UAT - User Acceptance Testing
UPS - Uninterruptable Power Supply
URL - Universal Resource Locator
USB – Universal Serial Bus
UTP – Unshielded Twisted Pair
VLAN – Virtual Local Area Network
VoIP - Voice over IP
VPN – Virtual Private Network
VTC – Video Teleconferencing
WAF- Web-Application Firewall
WAP – Wireless Access Point
WEP – Wired Equivalent Privacy
WIDS – Wireless Intrusion Detection System
WIPS – Wireless Intrusion Prevention System
WPA – Wireless Protected Access
XSRF - Cross-Site Request Forgery
XSRF- Cross-Site Request Forgery
XSS - Cross-Site Scripting