CompTIA Security+ Examination Objectives

Version 1.0

Introduction

The skills and knowledge measured by the CompTIA Security+ examination were derived and validated though input from a committee and over 1,000 subject matter experts representative of industry. A job task analysis (JTA), global survey, beta examination and beta results review were each milestones in the development process. The results of these milestones were used in weighing the domains and ensuring that the weighting assigned to each domain is representative of the relative importance of the content.

The CompTIA Security+ certification is an internationally recognized validation of the technical knowledge required of foundation-level security practitioners. A CompTIA Security+ certified individual has successfully proven holding a foundation-level of skill and knowledge in General Security Concepts, Communication Security, Infrastructure Security, Basics of Cryptography and Operational / Organizational Security. Candidates are recommended to have two years experience in a networking role with preexisting knowledge of TCP/IP, experience in a security related role, CompTIA Network+ or equivalent certification, and adequate training and self-study materials. All candidates are encouraged to review the CompTIA Security+ objectives thoroughly prior to attempting the exam.

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

The table below lists the domains measured by this examination and the extent to which they are represented in the examination. CompTIA Security+ (2007 Edition) exams are based on these objectives.

CompTIA Security+ Certification Domains	% of Exam*
1.0 General Security Concepts	30%
2.0 Communication Security	20%
3.0 Infrastructure Security	20%
4.0 Basics of Cryptography	15%
5.0 Operational / Organizational Security	15%

* All percentages are approximate and are subject to change.

CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

Domain 1.0 – General Security Concepts (30%)

1.1 Recognize and be able to differentiate and explain the following access control models
- MAC (Mandatory Access Control)
- DAC (Discretionary Access Control)
- RBAC (Role Based Access Control)

1.2 Recognize and be able to differentiate and explain the following methods of authentication
- Kerberos
- CHAP (Challenge Handshake Authentication Protocol)
- Certificates
- Username / Password
- Tokens
- Multi-factor
- Mutual
- Biometrics

1.3 Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols

1.4 Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk
- DOS / DDOS (Denial of Service / Distributed Denial of Service)
- Back Door
- Spoofing
- Man in the Middle
- Replay
- TCP/IP Hijacking
- Weak Keys
- Mathematical
- Social Engineering
- Birthday
- Password Guessing
  - Brute Force
  - Dictionary
- Software Exploitation

1.5 Recognize the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk
- Viruses
- Trojan Horses
- Logic Bombs
- Worms

1.6 Understand the concept of and know how to reduce the risks of social engineering

1.7 Understand the concept and significance of auditing, logging and system scanning

Domain 2.0 – Communication Security - 20%

2.1 Recognize and understand the administration of the following types of remote access technologies
- 802.1x
- VPN (Virtual Private Network)
- RADIUS (Remote Authentication Dial-In User Service)
- TACACS (Terminal Access Controller Access Control System)
- L2TP / PPTP (Layer Two Tunneling Protocol / Point to Point Tunneling Protocol)
- SSH (Secure Shell)
- IPSEC (Internet Protocol Security)
- Vulnerabilities

2.2 Recognize and understand the administration of the following email security concepts
- S/MIME (Secure Multipurpose Internet Mail Extensions)
- PGP (Pretty Good Privacy) like technologies
- Vulnerabilities
    - SPAM
    - Hoaxes

2.3 Recognize and understand the administration of the following Internet security concepts
- SSL / TLS (Secure Sockets Layer / Transport Layer Security)
- HTTP/S (Hypertext Transfer Protocol / Hypertext Transfer Protocol over Secure Sockets Layer)
- Instant Messaging
    - Vulnerabilities
    - Packet Sniffing
    - Privacy
- Vulnerabilities
    - Java Script
    - ActiveX
    - Buffer Overflows
    - Cookies
    - Signed Applets
    - CGI (Common Gateway Interface)
    - SMTP (Simple Mail Transfer Protocol) Relay

2.4 Recognize and understand the administration of the following directory security concepts
- SSL / TLS (Secure Sockets Layer / Transport Layer Security)
- LDAP (Lightweight Directory Access Protocol)

2.5 Recognize and understand the administration of the following file transfer protocols and concepts
- S/FTP (File Transfer Protocol)
- Blind FTP (File Transfer Protocol) / Anonymous
- File Sharing
- Vulnerabilities
    - Packet Sniffing
    - 8.3 Naming Conventions

2.6 Recognize and understand the administration of the following wireless technologies and concepts
- WTLS (Wireless Transport Layer Security)
- 802.11 and 802.11x
- WEP / WAP (Wired Equivalent Privacy / Wireless Application Protocol)

- Vulnerabilities
  - Site Surveys

Domain 3.0 Infrastructure Security – 20%

3.1 Understand security concerns and concepts of the following types of devices

- Firewalls
- Routers
- Switches
- Wireless
- Modems
- RAS (Remote Access Server)
- Telecom / PBX (Private Branch Exchange)
- VPN (Virtual Private Network)
- IDS (Intrusion Detection System)
- Network Monitoring / Diagnostics
- Workstations
- Servers
- Mobile Devices

3.2 Understand the security concerns for the following types of media

- Coaxial Cable
- UTP / STP (Unshielded Twisted Pair / Shielded Twisted Pair)
- Fiber Optic Cable
- Removable Media
  - Tape
  - CD-R (Recordable Compact Disks)
  - Hard Drives
  - Diskettes
  - Flashcards
  - Smartcards

3.3 Understand the concepts behind the following kinds of Security Topologies

- Security Zones
  - DMZ (Demilitarized Zone)
  - Intranet
  - Extranet
- VLANs (Virtual Local Area Network)
- NAT (Network Address Translation)
- Tunneling

3.4 Differentiate the following types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system

- Network Based
  - Active Detection
  - Passive Detection
- Host Based
  - Active Detection
  - Passive Detection
- Honey Pots
- Incident Response

3.5 Understand the following concepts of Security Baselines, be able to explain what a Security Baseline is, and understand the implementation and configuration of each kind of intrusion detection system

- OS / NOS (Operating System / Network Operating System) Hardening
  - File System

- Updates (Hotfixes, Service Packs, Patches)
- Network Hardening
  - Updates (Firmware)
  - Configuration
    - Enabling and Disabling Services and Protocols
    - Access Control Lists

- Application Hardening
  - Updates (Hotfixes, Service Packs, Patches)
  - Web Servers
  - E-mail Servers
  - FTP (File Transfer Protocol) Servers
  - DNS (Domain Name Service) Servers
  - NNTP (Network News Transfer Protocol) Servers
  - File / Print Servers
  - DHCP (Dynamic Host Configuration Protocol) Servers
  - Data Repositories
    - Directory Services
    - Databases

Domain 4.0 Basics of Cryptography – 15%

4.1 Be able to identify and explain each of the following different kinds of cryptographic algorithms

- Hashing
- Symmetric
- Asymmetric

4.2 Understand how cryptography addresses the following security concepts

- Confidentiality
- Integrity
  - Digital Signatures
- Authentication
- Non-Repudiation
  - Digital Signatures
- Access Control

4.3 Understand and be able to explain the following concepts of PKI (Public Key Infrastructure)

- Certificates
  - Certificate Policies
  - Certificate Practice Statements
- Revocation
- Trust Models

4.4 Identify and be able to differentiate different cryptographic standards and protocols

4.5 Understand and be able to explain the following concepts of Key Management and Certificate Lifecycles

- Centralized vs. Decentralized
- Storage
  - Hardware vs. Software
  - Private Key Protection
- Escrow
- Expiration
- Revocation
  - Status Checking
- Suspension
  - Status Checking
- Recovery
  - M-of-N Control (Of M appropriate individuals, N must be present to authorize recovery)
- Renewal
- Destruction
- Key Usage
  - Multiple Key Pairs (Single, Dual)

Domain 5.0 Operational / Organizational Security – 15%

5.1 Understand the application of the following concepts of physical security

- Access Control
  - Physical Barriers
  - Biometrics
- Social Engineering
- Environment
  - Wireless Cells
  - Location
  - Shielding
  - Fire Suppression

5.2 Understand the security implications of the following topics of disaster recovery

- Backups
  - Off Site Storage
- Secure Recovery
  - Alternate Sites
- Disaster Recovery Plan

5.3 Understand the security implications of the following topics of business continuity

- Utilities
- High Availability / Fault Tolerance
- Backups

5.4 Understand the concepts and uses of the following types of policies and procedures

- Security Policy
  - Acceptable Use
  - Due Care
  - Privacy
  - Separation of Duties
  - Need to Know
  - Password Management
  - SLAs (Service Level Agreements)
  - Disposal / Destruction
  - HR (Human Resources) Policy
    - Termination (Adding and revoking passwords and privileges, etc.)
    - Hiring (Adding and revoking passwords and privileges, etc.)
    - Code of Ethics
- Incident Response Policy

5.5 Explain the following concepts of privilege management

- User / Group / Role Management
- Single Sign-on
- Centralized vs. Decentralized
- Auditing (Privilege, Usage, Escalation)
- MAC / DAC / RBAC (Mandatory Access Control / Discretionary Access Control / Role Based Access Control)

5.6 Understand the concepts of the following topics of forensics

- Chain of Custody

- Preservation of Evidence
- Collection of Evidence

5.7 Understand and be able to explain the following concepts of risk identification
- Asset Identification
- Risk Assessment
- Threat Identification
- Vulnerabilities

5.8 Understand the security relevance of the education and training of end users, executives and human resources
- Communication
- User Awareness
- Education
- On-line Resources

5.9 Understand and explain the following documentation concepts
- Standards and Guidelines
- Systems Architecture
- Change Documentation
- Logs and Inventories
- Classification
  - Notification
- Retention / Storage
- Destruction