Certification Exam Objectives: SY0-201

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 skills and knowledge measured by this examination are derived from an industry-wide Job Task Analysis (JTA) and were validated through a global survey in Q4, 2007. The results of this survey were used to validate the content of the domains and objectives and the overall domain weightings, ensuring the relative importance of the content.

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

- A minimum of 2 years experience in network 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

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 Systems Security	21%
2.0 Network Infrastructure	20%
3.0 Access Control	17%
4.0 Assessments & Audits	15%
5.0 Cryptography	15%
6.0 Organizational Security	12%
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.

(A list of acronyms used in these Objectives appears at the end of this document.)

Objectives in italics are those objectives that contain content that has changed since the last version of the Security+ exam (2002 Objectives).

1.0 Systems Security

1.1 Differentiate among various systems security threats.

- Privilege escalation
- Virus
- Worm
- Trojan
- Spyware
- Spam
- Adware
- Rootkits
- Botnets
- Logic bomb

1.2 Explain the security risks pertaining to system hardware and peripherals.

- BIOS
- USB devices
- Cell phones
- Removable storage
- Network attached storage

1.3 Implement OS hardening practices and procedures to achieve workstation and server security.

- Hotfixes
- Service packs
- Patches
- Patch management
- Group policies
- Security templates
- Configuration baselines

1.4 Carry out the appropriate procedures to establish application security.

- ActiveX
- Java
- Scripting
- Browser
- Buffer overflows
- Cookies
- SMTP open relays
- Instant messaging
- P2P
- Input validation
- Cross-site scripting (XSS)

1.5 Implement security applications.

- HIDS
- Personal software firewalls
- Antivirus
- Anti-spam
- Popup blockers

1.6 Explain the purpose and application of virtualization technology.

2.0 Network Infrastructure

2.1 Differentiate between the different ports & protocols, their respective threats and mitigation techniques.

- Antiquated protocols
- TCP/IP hijacking
- Null sessions
- Spoofing
- Man-in-the-middle
- Replay
- DOS
- DDOS
- Domain Name Kiting
- DNS poisoning
- ARP poisoning

2.2 Distinguish between network design elements and components.

- DMZ
- VLAN
- NAT
- Network interconnections
- NAC
- Subnetting
- Telephony

2.3 Determine the appropriate use of network security tools to facilitate network security.

- NIDS
- NIPS
- Firewalls
- Proxy servers
- Honeypot
- Internet content filters
- Protocol analyzers

2.4 Apply the appropriate network tools to facilitate network security.

- NIDS
- Firewalls
- Proxy servers
- Internet content filters
- Protocol analyzers

2.5 Explain the vulnerabilities and mitigations associated with network devices.

- Privilege escalation
- Weak passwords
- Back doors
- Default accounts
- DOS

2.6 Explain the vulnerabilities and mitigations associated with various transmission media.

- Vampire taps

2.7 Explain the vulnerabilities and implement mitigations associated with wireless networking.

- Data emanation
- War driving
- SSID broadcast
- Blue jacking
- Bluesnarfing
- Rogue access points
- Weak encryption

3.0 Access Control

3.1 Identify and apply industry best practices for access control methods.

- Implicit deny
- Least privilege
- Separation of duties
- Job rotation

3.2 Explain common access control models and the differences between each.

- MAC
- DAC
- Role & Rule based access control

3.3 Organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges.

3.4 Apply appropriate security controls to file and print resources.

3.5 Compare and implement logical access control methods.

- ACL
- Group policies
- Password policy
- Domain password policy
- User names and passwords
- Time of day restrictions
- Account expiration
- Logical tokens

3.6 Summarize the various authentication models and identify the components of each.

- One, two and three-factor authentication
- Single sign-on

3.7 Deploy various authentication models and identify the components of each.

- Biometric reader
- RADIUS
- RAS
- LDAP
- Remote access policies
- Remote authentication
- VPN

- Kerberos
- CHAP
- PAP
- Mutual
- 802.1x
- TACACS

3.8 Explain the difference between identification and authentication (identity proofing).

3.9 Explain and apply physical access security methods.

- Physical access logs/lists
- Hardware locks
- Physical access control – ID badges
- Door access systems
- Man-trap
- Physical tokens
- Video surveillance – camera types and positioning

4.0 Assessments & Audits

4.1 Conduct risk assessments and implement risk mitigation.

4.2 Carry out vulnerability assessments using common tools.

- Port scanners
- Vulnerability scanners
- Protocol analyzers
- OVAL
- Password crackers
- Network mappers

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

4.4 Use monitoring tools on systems and networks and detect security-related anomalies.

- Performance monitor
- Systems monitor
- Performance baseline
- Protocol analyzers

4.5 Compare and contrast various types of monitoring methodologies.

- Behavior-based
- Signature-based
- Anomaly-based

4.6 Execute proper logging procedures and evaluate the results.

- Security application
- DNS
- System
- Performance
- Access

- Firewall
- Antivirus

4.7 Conduct periodic audits of system security settings.

- User access and rights review
- Storage and retention policies
- Group policies

5.0 Cryptography

5.1 Explain general cryptography concepts.

- Key management
- Steganography
- Symmetric key
- Asymmetric key
- Confidentiality
- Integrity and availability
- Non-repudiation
- Comparative strength of algorithms
- Digital signatures
- Whole disk encryption
- Trusted Platform Module (TPM)
- Single vs. Dual sided certificates
- Use of proven technologies

5.2 Explain basic hashing concepts and map various algorithms to appropriate applications.

- SHA
- MD5
- LANMAN
- NTLM

5.3 Explain basic encryption concepts and map various algorithms to appropriate applications.

- DES
- 3DES
- RSA
- PGP
- Elliptic curve
- AES
- AES256
- One time pad
- Transmission encryption (WEP TKIP, etc)

5.4 Explain and implement protocols.

- SSL/TLS
- S/MIME
- PPTP
- HTTP vs. HTTPS vs. SHTTP
- L2TP
- IPSEC
- SSH

5.5 Explain core concepts of public key cryptography.

- Public Key Infrastructure (PKI)
- Recovery agent
- Public key
- Private keys
- Certificate Authority (CA)
- Registration
- Key escrow
- Certificate Revocation List (CRL)
- Trust models

5.6 Implement PKI and certificate management.

- Public Key Infrastructure (PKI)
- Recovery agent
- Public key
- Private keys
- Certificate Authority (CA)
- Registration
- Key escrow
- Certificate Revocation List (CRL)

6.0 Organizational Security

6.1 Explain redundancy planning and its components.

- Hot site
- Cold site
- Warm site
- Backup generator
- Single point of failure
- RAID
- Spare parts
- Redundant servers
- Redundant ISP
- UPS
- Redundant connections

6.2 Implement disaster recovery procedures.

- Planning
- Disaster recovery exercises
- Backup techniques and practices – storage
- Schemes
- Restoration

6.3 Differentiate between and execute appropriate incident response procedures.

- Forensics
- Chain of custody
- First responders
- Damage and loss control
- Reporting – disclosure of

6.4 Identify and explain applicable legislation and organizational policies.

- Secure disposal of computers

- Acceptable use policies
- Password complexity
- Change management
- Classification of information
- Mandatory vacations
- Personally Identifiable Information (PII)
- Due care
- Due diligence
- Due process
- SLA
- Security-related HR policy
- User education and awareness training

6.5 Explain the importance of environmental controls.

- Fire suppression
- HVAC
- Shielding

6.6 Explain the concept of and how to reduce the risks of social engineering.

- Phishing
- Hoaxes
- Shoulder surfing
- Dumpster diving
- User education and awareness training

SECURITY+ ACRONYMS

3DES – Triple Digital Encryption Standard
ACL – Access Control List
AES - Advanced Encryption Standard
AES256 – Advanced Encryption Standards 256bit
AH - Authentication Header
ALE - Annualized Loss Expectancy
ARO - Annualized Rate of Occurrence
ARP - Address Resolution Protocol
AUP - Acceptable Use Policy
BIOS – Basic Input / Output System
BOTS – Network Robots
CA – Certificate Authority
CAN - Controller Area Network
CCTV - Closed-circuit television
CERT – Computer Emergency Response Team
CHAP – Challenge Handshake Authentication Protocol
CIRT – Computer Incident Response Team
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
DMZ – Demilitarized Zone
DNS – Domain Name Service (Server)
DOS – Denial of Service
DSA – Digital Signature Algorithm
EAP - Extensible Authentication Protocol
ECC - Elliptic Curve Cryptography
FTP – File Transfer Protocol
GRE - Generic Routing Encapsulation
HDD – Hard Disk Drive
HIDS – Host Based Intrusion Detection System
HIPS – Host Based Intrusion Prevention System
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol over SSL
HVAC – Heating, Ventilation Air Conditioning
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
KDC - Key Distribution Center
L2TP – Layer 2 Tunneling Protocol
LANMAN – Local Area Network Manager
LDAP – Lightweight Directory Access 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
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
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
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
S/MIME – Secure / Multipurpose internet Mail Extensions
SCSI - Small Computer System Interface
SHA – Secure Hashing Algorithm
SHTTP – Secure Hypertext Transfer Protocol
SIM – Subscriber Identity Module
SLA – Service Level Agreement
SLE - Single Loss Expectancy
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
TKIP – Temporal Key Interchange Protocol
TLS – Transport Layer Security
TPM – Trusted Platform Module
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
WAP – Wireless Access Point
WEP – Wired Equivalent Privacy
WIDS – Wireless Intrusion Detection System
WIPS – Wireless Intrusion Prevention System
WPA – Wi-Fi Protected Access