Certification Exam Objectives: SY0-401

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, to participate in risk mitigation activities, and to provide infrastructure, application, information, and operational security. In addition, the successful candidate will apply security controls to maintain confidentiality, integrity, and availability, identify appropriate technologies and products, troubleshoot security events and incidents, 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 accredited by ANSI to show compliance with the ISO 17024 Standard 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	20%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	20%
4.0 Application, Data and Host Security	15%
5.0 Access Control and Identity Management	15%
6.0 Cryptography	12%
Total	**100%**

CompTIA Authorized Materials Use Policy

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites, aka 'brain dumps'. Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies webpage:
http://certification.comptia.org/Training/testingcenters/policies.aspx

Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to
abide by the CompTIA Candidate Agreement
(http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx) at the time of exam delivery.

If a candidate has a question as to whether study materials are considered unauthorized (aka brain dumps), he/she should perform a search using CertGuard's
engine, found here:
http://www.certguard.com/search.asp

Or verify against this list:
http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx

**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.

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.

1.0 Network Security

1.1 Implement security configuration parameters on network devices and other technologies.

- Firewalls
- Routers
- Switches
- Load Balancers
- Proxies
- Web security gateways
- VPN concentrators
- NIDS and NIPS
  - Behavior based
  - Signature based
  - Anomaly based
  - Heuristic
- Protocol analyzers
- Spam filter
- UTM security appliances
  - URL filter
  - Content inspection
  - Malware inspection
- Web application firewall vs. network firewall
- Application aware devices
  - Firewalls
  - IPS
  - IDS
  - Proxies

1.2 Given a scenario, use 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
- Network separation
- Log analysis
- Unified Threat Management

1.3 Explain network design elements and components.

- DMZ
- Subnetting
- VLAN
- NAT
- Remote Access
- Telephony

- NAC
- Virtualization
- Cloud Computing
    - Platform as a Service
    - Software as a Service
    - Infrastructure as a Service
    - Private
    - Public
    - Hybrid
    - Community
- Layered security / Defense in depth

1.4 Given a scenario, implement common protocols and services.

- Protocols
    - IPSec
    - SNMP
    - SSH
    - DNS
    - TLS
    - SSL
    - TCP/IP
    - FTPS
    - HTTPS
    - SCP
    - ICMP
    - IPv4
    - IPv6
    - iSCSI
    - Fibre Channel
    - FCoE
    - FTP
    - SFTP
    - TFTP
    - TELNET
    - HTTP
    - NetBIOS
- Ports
    - 21
    - 22
    - 25
    - 53
    - 80
    - 110
    - 139
    - 143
    - 443
    - 3389
- OSI relevance

1.5 Given a scenario, troubleshoot security issues related to wireless networking.

- WPA
- WPA2
- WEP

- EAP
- PEAP
- LEAP
- MAC filter
- Disable SSID broadcast
- TKIP
- CCMP
- Antenna Placement
- Power level controls
- Captive portals
- Antenna types
- Site surveys
- VPN (over open wireless)

2.0 Compliance and Operational Security

2.1 Explain the importance of risk related concepts.

- Control types
  - Technical
  - Management
  - Operational
- False positives
- False negatives
- 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
  - SLE
  - ARO
  - MTTR
  - MTTF
  - MTBF
- Quantitative vs. qualitative
- Vulnerabilities
- Threat vectors
- Probability / threat likelihood
- Risk-avoidance, transference, acceptance, mitigation, deterrence
- Risks associated with Cloud Computing and Virtualization
- Recovery time objective and recovery point objective

2.2 Summarize the security implications of integrating systems and data with third parties.

- On-boarding/off-boarding business partners
- Social media networks and/or applications
- Interoperability agreements

    - SLA
    - BPA
    - MOU
    - ISA
- Privacy considerations
- Risk awareness
- Unauthorized data sharing
- Data ownership
- Data backups
- Follow security policy and procedures
- Review agreement requirements to verify compliance and performance standards

2.3 Given a scenario, implement appropriate risk mitigation strategies.

- Change management
- Incident management
- User rights and permissions reviews
- Perform routine audits
- Enforce policies and procedures to prevent data loss or theft
- Enforce technology controls
    - Data Loss Prevention (DLP)

2.4 Given a scenario, implement 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
- Chain of custody
- Big Data analysis

2.5 Summarize common incident response procedures.

- Preparation
- Incident identification
- Escalation and notification
- Mitigation steps
- Lessons learned
- Reporting
- Recovery/reconstitution procedures
- First responder
- Incident isolation
    - Quarantine
    - Device removal
- Data breach
- Damage and loss control

2.6 Explain the importance of security related awareness and training.

- Security policy training and procedures
- Role-based training

- Personally identifiable information
- Information classification
    - High
    - Medium
    - Low
    - Confidential
    - Private
    - Public
- 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
- New threats and new security trends/alerts
    - New viruses
    - Phishing attacks
    - Zero-day exploits
- Use of social networking and P2P
- Follow up and gather training metrics to validate compliance and security posture

2.7 Compare and contrast physical security and environmental controls.

- Environmental controls
    - HVAC
    - Fire suppression
    - EMI shielding
    - Hot and cold aisles
    - Environmental monitoring
    - Temperature and humidity controls
- Physical security
    - Hardware locks
    - Mantraps
    - Video Surveillance
    - Fencing
    - Proximity readers
    - Access list
    - Proper lighting
    - Signs
    - Guards
    - Barricades
    - Biometrics
    - Protected distribution (cabling)
    - Alarms
    - Motion detection
- Control types
    - Deterrent
    - Preventive
    - Detective
    - Compensating
    - Technical
    - Administrative

2.8 Summarize risk management best practices.

- Business continuity concepts
  - Business impact analysis
  - Identification of critical systems and components
  - Removing single points of failure
  - Business continuity planning and testing
  - Risk assessment
  - Continuity of operations
  - Disaster recovery
  - IT contingency planning
  - Succession planning
  - High availability
  - Redundancy
  - Tabletop exercises
- Fault tolerance
  - Hardware
  - RAID
  - Clustering
  - Load balancing
  - Servers
- Disaster recovery concepts
  - Backup plans/policies
  - Backup execution/frequency
  - Cold site
  - Hot site
  - Warm site

2.9 Given a scenario, select the appropriate control to meet the goals of security.

- Confidentiality
  - Encryption
  - Access controls
  - Steganography
- Integrity
  - Hashing
  - Digital signatures
  - Certificates
  - Non-repudiation
- Availability
  - Redundancy
  - Fault tolerance
  - Patching
- Safety
  - Fencing
  - Lighting
  - Locks
  - CCTV
  - Escape plans
  - Drills
  - Escape routes
  - Testing controls

3.0 Threats and Vulnerabilities

3.1 Explain types of malware.

- Adware
- Virus
- Spyware
- Trojan
- Rootkits
- Backdoors
- Logic bomb
- Botnets
- Ransomware
- Polymorphic malware
- Armored virus

3.2 Summarize various 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
- Password attacks
    - Brute force
    - Dictionary attacks
    - Hybrid
    - Birthday attacks
    - Rainbow tables
- Typo squatting/URL hijacking
- Watering hole attack

3.3 Summarize social engineering attacks and the associated effectiveness with each attack.

- Shoulder surfing
- Dumpster diving
- Tailgating
- Impersonation
- Hoaxes
- Whaling
- Vishing
- Principles (reasons for effectiveness)
    - Authority
    - Intimidation
    - Consensus/Social proof

- Scarcity
- Urgency
- Familiarity/liking
- Trust

3.4 Explain types of wireless attacks.

- Rogue access points
- Jamming/Interference
- Evil twin
- War driving
- Bluejacking
- Bluesnarfing
- War chalking
- IV attack
- Packet sniffing
- Near field communication
- Replay attacks
- WEP/WPA attacks
- WPS attacks

3.5 Explain types of application attacks.

- Cross-site scripting
- SQL injection
- LDAP injection
- XML injection
- Directory traversal/command injection
- Buffer overflow
- Integer overflow
- Zero-day
- Cookies and attachments
- LSO (Locally Shared Objects)
- Flash Cookies
- Malicious add-ons
- Session hijacking
- Header manipulation
- Arbitrary code execution / remote code execution

3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.

- Monitoring system logs
  - Event logs
  - Audit logs
  - Security logs
  - Access logs
- Hardening
  - Disabling unnecessary services
  - Protecting management interfaces and applications
  - Password protection
  - Disabling unnecessary accounts
- Network security
  - MAC limiting and filtering
  - 802.1x
  - Disabling unused interfaces and unused application service ports

    - Rogue machine detection
- 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 Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.

- Interpret results of security assessment tools
- Tools
    - Protocol analyzer
    - Vulnerability scanner
    - Honeypots
    - Honeynets
    - Port scanner
    - Passive vs. active tools
    - Banner grabbing
- Risk calculations
    - Threat vs. likelihood
- Assessment types
    - Risk
    - Threat
    - Vulnerability
- Assessment technique
    - Baseline reporting
    - Code review
    - Determine attack surface
    - Review architecture
    - Review designs

3.8 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
    - Identify vulnerability
    - Identify lack of security controls
    - Identify common misconfigurations
    - Intrusive vs. non-intrusive
    - Credentialed vs. non-credentialed
    - False positive
- Black box
- White box
- Gray box

4.0 Application, Data and Host Security

4.1 Explain the importance of application security controls and techniques.

- 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
- NoSQL databases vs. SQL databases
- Server-side vs. Client-side validation

4.2 Summarize mobile security concepts and technologies.

- Device security
  - Full device encryption
  - Remote wiping
  - Lockout
  - Screen-locks
  - GPS
  - Application control
  - Storage segmentation
  - Asset tracking
  - Inventory control
  - Mobile device management
  - Device access control
  - Removable storage
  - Disabling unused features
- Application security
  - Key management
  - Credential management
  - Authentication
  - Geo-tagging
  - Encryption
  - Application whitelisting
  - Transitive trust/authentication
- BYOD concerns
  - Data ownership
  - Support ownership
  - Patch management
  - Antivirus management
  - Forensics
  - Privacy
  - On-boarding/off-boarding
  - Adherence to corporate policies
  - User acceptance
  - Architecture/infrastructure considerations
  - Legal concerns
  - Acceptable use policy
  - On-board camera/video

4.3 Given a scenario, select the appropriate solution to establish host security.

- Operating system security and settings
- OS hardening
- Anti-malware
  - Antivirus
  - Anti-spam
  - Anti-spyware
  - Pop-up blockers
- Patch management
- White listing vs. black listing applications
- Trusted OS
- Host-based firewalls
- Host-based intrusion detection
- Hardware security
  - Cable locks
  - Safe
  - Locking cabinets
- Host software baselining
- Virtualization
  - Snapshots
  - Patch compatibility
  - Host availability/elasticity
  - Security control testing
  - Sandboxing

4.4 Implement the appropriate controls to ensure data security.

- Cloud storage
- SAN
- Handling Big Data
- Data encryption
  - Full disk
  - Database
  - Individual files
  - Removable media
  - Mobile devices
- Hardware based encryption devices
  - TPM
  - HSM
  - USB encryption
  - Hard drive
- Data in-transit, Data at-rest, Data in-use
- Permissions/ACL
- Data policies
  - Wiping
  - Disposing
  - Retention
  - Storage

4.5 Compare and contrast alternative methods to mitigate security risks in static environments.

- Environments
  - SCADA
  - Embedded (Printer, Smart TV, HVAC control)
  - Android

    - iOS
    - Mainframe
    - Game consoles
    - In-vehicle computing systems
- Methods
    - Network segmentation
    - Security layers
    - Application firewalls
    - Manual updates
    - Firmware version control
    - Wrappers
    - Control redundancy and diversity

5.0 Access Control and Identity Management

5.1 Compare and contrast the function and purpose of authentication services.

- RADIUS
- TACACS+
- Kerberos
- LDAP
- XTACACS
- SAML
- Secure LDAP

5.2 Given a scenario, select the appropriate authentication, authorization or access control.

- Identification vs. authentication vs. authorization
- Authorization
    - Least privilege
    - Separation of duties
    - ACLs
    - Mandatory access
    - Discretionary access
    - Rule-based access control
    - Role-based access control
    - Time of day restrictions
- Authentication
    - Tokens
    - Common access card
    - Smart card
    - Multifactor authentication
    - TOTP
    - HOTP
    - CHAP
    - PAP
    - Single sign-on
    - Access control
    - Implicit deny
    - Trusted OS
- Authentication factors
    - Something you are
    - Something you have
    - Something you know
    - Somewhere you are

    - Something you do
- Identification
    - Biometrics
    - Personal identification verification card
    - Username
- Federation
- Transitive trust/authentication

5.3 Install and configure security controls when performing account management, based on best practices.

- Mitigate issues associated with users with multiple account/roles and/or shared accounts
- Account policy enforcement
    - Credential management
    - Group policy
    - Password complexity
    - Expiration
    - Recovery
    - Disablement
    - Lockout
    - Password history
    - Password reuse
    - Password length
    - Generic account prohibition
- Group based privileges
- User assigned privileges
- User access reviews
- Continuous monitoring

6.0 Cryptography

6.1 Given a scenario, utilize general cryptography concepts.

- Symmetric vs. asymmetric
- Session keys
- In-band vs. out-of-band key exchange
- 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
- Ephemeral key
- Perfect forward secrecy

6.2 Given a scenario, use appropriate cryptographic methods.

- WEP vs. WPA/WPA2 and preshared key
- MD5
- SHA

- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA
- Diffie-Hellman
- RC4
- One-time pads
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- TwoFish
- DHE
- ECDHE
- CHAP
- PAP
- Comparative strengths and performance of algorithms
- Use of algorithms/protocols with transport encryption
    - SSL
    - TLS
    - IPSec
    - SSH
    - HTTPS
- Cipher suites
    - Strong vs. weak ciphers
- Key stretching
    - PBKDF2
    - Bcrypt

6.3 Given a scenario, use appropriate PKI, certificate management and associated components.

- Certificate authorities and digital certificates
    - CA
    - CRLs
    - OCSP
    - CSR
- PKI
- Recovery agent
- Public key
- Private key
- 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
API - Application Programming Interface
ASP - Application Service Provider
ARO - Annualized Rate of Occurrence
ARP - Address Resolution Protocol
AUP - Acceptable Use Policy
BAC – Business Availability Center
BCP – Business Continuity Planning
BIA- Business Impact Analysis
BIOS – Basic Input / Output System
BPA – Business Partners Agreement
BYOD – Bring Your Own Device
CA – Certificate Authority
CAC - Common Access Card
CAN - Controller Area Network
CAPTCHA- Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAR- Corrective Action Report
CCMP – Counter-Mode/CBC-Mac Protocol
CCTV - Closed-circuit television
CERT – Computer Emergency Response Team
CHAP – Challenge Handshake Authentication Protocol
CIO-- Chief Information Officer
CIRT – Computer Incident Response Team
COOP – Continuity of Operation Planning
CP – Contingency Planning
CRC – Cyclical Redundancy Check
CRL – Certification Revocation List
CSR – Control Status Register
CSU – Channel Service Unit
CTO- Chief Technology Officer
DAC – Discretionary Access Control

DBA– Database Administrator
DDOS – Distributed Denial of Service
DEP – Data Execution Prevention
DES – Digital Encryption Standard
DHCP – Dynamic Host Configuration Protocol
DHE – Data-Handling Electronics
DHE - Diffie-Hellman Ephemeral
DLL - Dynamic Link Library
DLP - Data Loss Prevention
DMZ – Demilitarized Zone
DNAT – Destination Network Address Transaction
DNS – Domain Name Service (Server)
DOS – Denial of Service
DRP – Disaster Recovery Plan
DSA – Digital Signature Algorithm
DSL - Digital Subscriber line
DSU – Data Service Unit
EAP - Extensible Authentication Protocol
ECC - Elliptic Curve Cryptography
ECDHE – Elliptic Curve Diffie-Hellman Ephemeral
EFS – Encrypted File System
EMI – Electromagnetic Interference
ESN- Electronic Serial Number
ESP – Encapsulated Security Payload
FACL- File System Access Control List
FDE– Full Disk Encryption
FTP – File Transfer Protocol
FTPS – Secured File Transfer Protocol
GPG – Gnu Privacy Guard
GPO – Group Policy Object
GPS – Global Positioning System
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
HOTP – HMAC based One Time Password
HSM – Hardware Security Module
HTML – HyperText Markup Language
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
IDS – Intrusion Detection System
IKE – Internet Key Exchange
IM - Instant messaging
IMAP4 - Internet Message Access Protocol v4
IP - Internet Protocol
IPSEC – Internet Protocol Security
IR– Incident Response
IRC - Internet Relay Chat
IRP – Incident Response Procedure
ISA – Interconnection Security Agreement
ISP – Internet Service Provider
ISSO- Information Systems Security Officer
ITCP – IT Contingency Plan
IV - Initialization Vector
JBOD– Just a Bunch of Disks
KDC - Key Distribution Center
L2TP – Layer 2 Tunneling Protocol
LAN – Local Area Network
LDAP – Lightweight Directory Access Protocol
LEAP – Lightweight Extensible Authentication Protocol
MaaS- Monitoring as a Service
MAC – Mandatory Access Control / Media Access Control
MAC - Message Authentication Code
MAN - Metropolitan Area Network
MBR – Master Boot Record
MD5 – Message Digest 5
MOU – Memorandum of Understanding
MPLS – Multi-Protocol Layer Switch
MSCHAP – Microsoft Challenge Handshake Authentication Protocol
MTBF – Mean Time Between Failures
MTTR – Mean Time to Recover
MTTF – Mean Time to Failure
MTU - Maximum Transmission Unit
NAC – Network Access Control
NAT – Network Address Translation
NDA – Non-Disclosure Agreement
NFC– Near Field Communication
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
OCSP – Online Certificate Status Protocol
OLA – Open License Agreement
OS – Operating System
OVAL – Open Vulnerability Assessment Language
P2P – Peer to Peer
PAC– Proxy Auto Configuration
PAM – Pluggable Authentication Modules
PAP – Password Authentication Protocol
PAT - Port Address Translation
PBKDF2 – Password Based Key Derivation Function 2
PBX – Private Branch Exchange
PCAP – Packet Capture
PEAP – Protected Extensible Authentication Protocol
PED - Personal Electronic Device
PGP – Pretty Good Privacy
PII – Personally Identifiable Information
PIV – Personal Identity Verification
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
RC4 – RSA Variable Key Size Encryption Algorithm
RIPEMD – RACE Integrity Primitives Evaluation Message Digest
ROI – Return of Investment
RPO – Recovery Point Objective
RSA – Rivest, Shamir, & Adleman
RTO – Recovery Time Objective

RTP – Real-Time Transport Protocol
S/MIME – Secure / Multipurpose Internet Mail Extensions
SAML – Security Assertions Markup Language
SaaS - Software as a Service
SAN – Storage Area Network
SCADA – System Control and Data Acquisition
SCAP - Security Content Automation Protocol
SCEP- Simple Certificate Enrollment Protocol
SCSI - Small Computer System Interface
SDLC - Software Development Life Cycle
SDLM - Software Development Life Cycle Methodology
SEH – Structured Exception Handler
SHA – Secure Hashing Algorithm
SFTP – Secured File Transfer Protocol
SHTTP – Secure Hypertext Transfer Protocol
SIEM – Security Information and Event Management
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
SOAP – Simple Object Access Protocol
SONET – Synchronous Optical Network Technologies
SPIM - Spam over Internet Messaging
SQL – Structured Query Language
SSD – Solid State Drive
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
TGT– Ticket Granting Ticket
TKIP - Temporal Key Integrity Protocol
TLS – Transport Layer Security
TOTP – Time-Based One-Time Password
TPM – Trusted Platform Module
TSIG – Transaction Signature
UAT - User Acceptance Testing
UEFI – Unified Extensible Firmware Interface
UDP- User Datagram Protocol

UPS - Uninterruptable Power Supply
URI- Uniform Resource Identifier
URL - Universal Resource Locator
USB – Universal Serial Bus
UTM- Unified Threat Management
UTP – Unshielded Twisted Pair
VDI – Virtualization Desktop Infrastructure
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
WPA2 – WiFi Protected Access 2
WPS – WiFi Protected Setup
WTLS – Wireless TLS
XML – Extensible Markup Language
XSRF- Cross-Site Request Forgery
XSS - Cross-Site Scripting

Suggested Classroom Equipment to have for Security+ Certification Training Equipment

- Router
- Firewall
- Access point
- Switch
- IDS/IPS
- Server
- Content filter
- Client
- Mobile device
- VPN concentrator
- All in one appliance
- Enterprise security managers / SIEM suite
- Load balancer

Spare parts/hardware

- Keyboards, mice
- Network cables
- Monitors

Tools

- WiFi analyzers

Software

- Backtrack
- Proxy server
- Kali/BackTrack
- Virtualization software
- Virtualized appliances
- Wireshark
- TCPdump
- NMAP
- OpenVAS
- Metasploit
- Backorifice
- Cain & Abel
- John the Ripper
- PF Sense
- Security Onion
- Roo
- Any UTM

Other

- Source Forge