CompTIA Security+ Certification Exam Objectives

EXAM NUMBER: SY0-501

CompTIA

About the Exam

The CompTIA Security+ certification is a vendor-neutral credential. The CompTIA Security+ SY0-501 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 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**
- **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.

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

- **A minimum of two 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**

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all content in this examination.

EXAM ACCREDITATION

CompTIA Security+ is accredited by ANSI to show compliance with the ISO 17024 standard and, as such, the exam objectives undergo regular reviews and updates.

EXAM DEVELOPMENT

CompTIA exams result from subject-matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

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**. 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**. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format 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.

TEST DETAILS

Required exam	SY0-501
Number of questions	Maximum of 90
Types of questions	Multiple choice and performance-based
Length of test	90 minutes
Recommended experience	At least two years of experience in IT administration with a focus on security
Passing score	750 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented:

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Threats, Attacks and Vulnerabilities	21%
2.0 Technologies and Tools	22%
3.0 Architecture and Design	15%
4.0 Identity and Access Management	16%
5.0 Risk Management	14%
6.0 Cryptography and PKI	12%
Total	**100%**

1.0 Threats, Attacks and Vulnerabilities

1.1 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**

1.2 Compare and contrast types of attacks.

- **Social engineering**
  - Phishing
  - Spear phishing
  - Whaling
  - Vishing
  - Tailgating
  - Impersonation
  - Dumpster diving
  - Shoulder surfing
  - Hoax
  - Watering hole attack
  - Principles (reasons for effectiveness)
    - Authority
    - Intimidation
    - Consensus
    - Scarcity
    - Familiarity
    - Trust
    - Urgency
- **Application/service attacks**
  - DoS
  - DDoS
  - On-path attack (previously known as man-in-the-middle attack/man-in-the-browser attack)
  - Buffer overflow
  - Injection
  - Cross-site scripting
  - Cross-site request forgery
  - Privilege escalation
  - ARP poisoning
  - Amplification
  - DNS poisoning
  - Domain hijacking
  - Zero day
  - Replay
  - Pass the hash
  - Hijacking and related attacks
    - Clickjacking
    - Session hijacking
    - URL hijacking
    - Typo squatting
  - Driver manipulation
    - Shimming
    - Refactoring
  - MAC spoofing
  - IP spoofing
- **Wireless attacks**
  - Replay
  - IV
  - Evil twin
  - Rogue AP
  - Jamming
  - WPS
  - Bluejacking
  - Bluesnarfing
  - RFID
  - NFC
  - Disassociation
- **Cryptographic attacks**
  - Birthday
  - Known plain text/cipher text
  - Rainbow tables
  - Dictionary
  - Brute force
    - Online vs. offline
  - Collision
  - Downgrade
  - Replay
  - Weak implementations

1.3 Explain threat actor types and attributes.

- **Types of actors**
  - Script kiddies
  - Hacktivist
  - Organized crime
  - Nation states/APT
  - Insiders
  - Competitors
- **Attributes of actors**
  - Internal/external
  - Level of sophistication
  - Resources/funding
  - Intent/motivation
- **Use of open-source intelligence**

1.4 Explain penetration testing concepts.

- **Active reconnaissance**
- **Passive reconnaissance**
- **Pivot**
- **Initial exploitation**
- **Persistence**
- **Escalation of privilege**
- **Unknown environment**
- **Known environment**
- **Partially known environment**
- **Penetration testing vs. vulnerability scanning**

1.5 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**

1.6 Explain the impact associated with types of vulnerabilities.

- **Race conditions**
- **Vulnerabilities due to:**
  - End-of-life systems
  - Embedded systems
  - Lack of vendor support
- **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**
  - Memory leak
  - Integer overflow
  - Buffer overflow
  - Pointer dereference
  - DLL injection
- **System sprawl/undocumented assets**
- **Architecture/design weaknesses**
- **New threats/zero day**
- **Improper certificate and key management**

2.0 Technologies and Tools

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- **Firewall**
  - ACL
  - Application-based vs. network-based
  - Stateful vs. stateless
  - Implicit deny
- **VPN concentrator**
  - Remote access vs. site-to-site
  - IPSec
    - Tunnel mode
    - Transport mode
    - AH
    - ESP
  - Split tunnel vs. full tunnel
  - TLS
  - Always-on VPN
- **NIPS/NIDS**
  - Signature-based
  - Heuristic/behavioral
  - Anomaly
  - Inline vs. passive
  - In-band vs. out-of-band
  - Rules
  - Analytics
    - False positive
    - False negative
- **Router**
  - ACLs
  - Antispoofing
- **Switch**
  - Port security
  - Layer 2 vs. Layer 3
  - Loop prevention
  - Flood guard
- **Proxy**
  - Forward and reverse proxy
  - Transparent
  - Application/multipurpose
- **Load balancer**
  - Scheduling
    - Affinity
    - Round-robin
  - Active-passive
  - Active-active
  - Virtual IPs
- **Access point**
  - SSID
  - MAC filtering
  - Signal strength
  - Band selection/width
  - Antenna types and placement
  - Fat vs. thin
  - Controller-based vs. standalone
- **SIEM**
  - Aggregation
  - Correlation
  - Automated alerting and triggers
  - Time synchronization
  - Event deduplication
  - Logs/WORM
- **DLP**
  - USB blocking
  - Cloud-based
  - Email
- **NAC**
  - Dissolvable vs. permanent
  - Host health checks
  - Agent vs. agentless
- **Mail gateway**
  - Spam filter
  - DLP
  - Encryption
- **Bridge**
- **SSL/TLS accelerators**
- **SSL decryptors**
- **Media gateway**
- **Hardware security module**

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- **Protocol analyzer**
- **Network scanners**
  - Rogue system detection
  - Network mapping
- **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**
  - ping
  - netstat
  - tracert
  - nslookup/dig
  - arp
  - ipconfig/ip/ifconfig
  - tcpdump
  - nmap
  - netcat

CompTIA

2.3 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**
  - Firewall
  - Content filter
  - Access points
- **Weak security configurations**
- **Personnel issues**
  - Policy violation
  - Insider threat
  - Social engineering
  - Social media
  - Personal email
- **Unauthorized software**
- **Baseline deviation**
- **License compliance violation (availability/integrity)**
- **Asset management**
- **Authentication issues**

2.4 Given a scenario, analyze and interpret output from security technologies.

- **HIDS/HIPS**
- **Antivirus**
- **File integrity check**
- **Host-based firewall**
- **Application allow list**
- **Removable media control**
- **Advanced malware tools**
- **Patch management tools**
- **UTM**
- **DLP**
- **Data execution prevention**
- **Web application firewall**

2.5 Given a scenario, deploy mobile devices securely.

- **Connection methods**
  - Cellular
  - WiFi
  - SATCOM
  - Bluetooth
  - NFC
  - ANT
  - Infrared
  - USB
- **Mobile device management concepts**
  - Application management
  - Content management
  - Remote wipe
  - Geofencing
  - Geolocation
  - Screen locks
  - Push notification services
  - Passwords and pins
  - Biometrics
  - Context-aware authentication
  - Containerization
  - Storage segmentation
  - Full device encryption
- **Enforcement and monitoring for:**
  - Third-party app stores
  - Rooting/jailbreaking
  - Sideloading
  - Custom firmware
  - Carrier unlocking
  - Firmware OTA updates
  - Camera use
  - SMS/MMS
  - External media
  - USB OTG
  - Recording microphone
  - GPS tagging
  - WiFi direct/ad hoc
  - Tethering
  - Payment methods
- **Deployment models**
  - BYOD
  - COPE
  - CYOD
  - Corporate-owned
  - VDI

2.6 Given a scenario, implement secure protocols.

- **Protocols**
  - DNSSEC
  - SSH
  - S/MIME
  - SRTP
  - LDAPS
  - FTPS
  - SFTP
  - SNMPv3
  - SSL/TLS
  - HTTPS
  - Secure POP/IMAP
- **Use cases**
  - Voice and video
  - Time synchronization
  - Email and web
  - File transfer
  - Directory services
  - Remote access
  - Domain name resolution
  - Routing and switching
  - Network address allocation
  - Subscription services

3.0 Architecture and Design

3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.

- **Industry-standard frameworks and reference architectures**
  - Regulatory
  - Non-regulatory
  - National vs. international
  - Industry-specific frameworks
- **Benchmarks/secure configuration guides**
  - Platform/vendor-specific guides
    - Web server
    - Operating system
    - Application server
    - Network infrastructure devices
  - General purpose guides
- **Defense-in-depth/layered security**
  - Vendor diversity
  - Control diversity
    - Administrative
    - Technical
  - User training

3.2 Given a scenario, implement secure network architecture concepts.

- **Zones/topologies**
  - Screened subnet (previously knwon as demilitarized zone)
  - Extranet
  - Intranet
  - Wireless
  - Guest
  - Honeynets
  - NAT
  - Ad hoc
- **Segregation/segmentation/isolation**
  - Physical
  - Logical (VLAN)
  - Virtualization
  - Air gaps
- **Tunneling/VPN**
  - Site-to-site
  - Remote access
- **Security device/technology placement**
  - Sensors
  - Collectors
  - Correlation engines
  - Filters
  - Proxies
  - Firewalls
  - VPN concentrators
  - SSL accelerators
  - Load balancers
  - DDoS mitigator
  - Aggregation switches
  - Taps and port mirror
- **SDN**

3.3 Given a scenario, implement secure systems design.

- **Hardware/firmware security**
  - FDE/SED
  - TPM
  - HSM
  - UEFI/BIOS
  - Secure boot and attestation
  - Supply chain
  - Hardware root of trust
  - EMI/EMP
- **Operating systems**
  - Types
    - Network
    - Server
    - Workstation
    - Appliance
    - Kiosk
    - Mobile OS
  - Patch management
  - Disabling unnecessary ports and services
  - Least functionality
  - Secure configurations
  - Trusted operating system
  - Application allow list/deny list
  - Disable default accounts/passwords
- **Peripherals**
  - Wireless keyboards
  - Wireless mice
  - Displays
  - WiFi-enabled MicroSD cards
  - Printers/MFDs
  - External storage devices
  - Digital cameras

CompTIA

3.4 Explain the importance of secure staging deployment concepts.

- **Sandboxing**
- **Environment**
  - Development
  - Test
  - Staging
  - Production
- **Secure baseline**
- **Integrity measurement**

3.5 Explain the security implications of embedded systems.

- **SCADA/ICS**
- **Smart devices/IoT**
  - Wearable technology
  - Home automation
- **HVAC**
- **SoC**
- **RTOS**
- **Printers/MFDs**
- **Camera systems**
- **Special purpose**
  - Medical devices
  - Vehicles
  - Aircraft/UAV

3.6 Summarize secure application development and deployment concepts.

- **Development life-cycle models**
  - Waterfall vs. Agile
- **Secure DevOps**
  - Security automation
  - Continuous integration
  - Baselining
  - Immutable systems
  - Infrastructure as code
- **Version control and change management**
- **Provisioning and deprovisioning**
- **Secure coding techniques**
  - Proper error handling
  - Proper input validation
  - Normalization
  - Stored procedures
  - Code signing
  - Encryption
  - Obfuscation/camouflage
  - Code reuse/dead code
  - Server-side vs. client-side execution and validation
  - Memory management
  - Use of third-party libraries and SDKs
  - Data exposure
- **Code quality and testing**
  - Static code analyzers
  - Dynamic analysis (e.g., fuzzing)
  - Stress testing
  - Sandboxing
  - Model verification
- **Compiled vs. runtime code**

3.7 Summarize cloud and virtualization concepts.

- **Hypervisor**
  - Type I
  - Type II
  - Application cells/containers
- **VM sprawl avoidance**
- **VM escape protection**
- **Cloud storage**
- **Cloud deployment models**
  - SaaS
  - PaaS
  - IaaS
  - Private
  - Public
  - Hybrid
  - Community
- **On-premise vs. hosted vs. cloud**
- **VDI/VDE**
- **Cloud access security broker**
- **Security as a service**

3.8 Explain how resiliency and automation strategies reduce risk.

- **Automation/scripting**
  - Automated courses of action
  - Continuous monitoring
  - Configuration validation
- **Templates**
- **Master image**
- **Non-persistence**
  - Snapshots
  - Revert to known state
  - Rollback to known configuration
  - Live boot media
- **Elasticity**
- **Scalability**
- **Distributive allocation**
- **Redundancy**
- **Fault tolerance**
- **High availability**
- **RAID**

3.9 Explain the importance of physical security controls.

- **Lighting**
- **Signs**
- **Fencing/gate/cage**
- **Security guards**
- **Alarms**
- **Safe**
- **Secure cabinets/enclosures**
- **Protected distribution/Protected cabling**
- **Airgap**
- **Access control vestibule**
- **Faraday cage**
- **Lock types**
- **Biometrics**
- **Barricades/bollards**
- **Tokens/cards**
- **Environmental controls**
  - HVAC
  - Hot and cold aisles
  - Fire suppression
- **Cable locks**
- **Screen filters**
- **Cameras**
- **Motion detection**
- **Logs**
- **Infrared detection**
- **Key management**

4.0 Identity and Access Management

4.1 Compare and contrast identity and access management concepts

- **Identification, authentication, authorization and accounting (AAA)**
- **Multifactor authentication**
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- **Federation**
- **Single sign-on**
- **Transitive trust**

4.2 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**

4.3 Given a scenario, implement identity and access management controls.

- **Access control models**
  - MAC
  - DAC
  - ABAC
  - Role-based access control
  - Rule-based access control
- **Physical access control**
  - Proximity cards
  - Smart cards
- **Biometric factors**
  - Fingerprint scanner
  - Retinal scanner
  - Iris scanner
  - Voice recognition
  - Facial recognition
  - False acceptance rate
  - False rejection rate
  - Crossover error rate
- **Tokens**
  - Hardware
  - Software
  - HOTP/TOTP
- **Certificate-based authentication**
  - PIV/CAC/smart card
  - IEEE 802.1x
- **File system security**
- **Database security**

4.4 Given a scenario, differentiate common account management practices.

- **Account types**
  - User account
  - Shared and generic accounts/credentials
  - Guest accounts
  - Service accounts
  - Privileged accounts
- **General Concepts**
  - Least privilege
  - Onboarding/offboarding
  - Permission auditing and review
  - Usage auditing and review
  - Time-of-day restrictions
  - Recertification
  - Standard naming convention
  - Account maintenance
  - Group-based access control
  - Location-based policies
- **Account policy enforcement**
  - Credential management
  - Group policy
  - Password complexity
  - Expiration
  - Recovery
  - Disablement
  - Lockout
  - Password history
  - Password reuse
  - Password length

CompTIA.

5.0 Risk Management

5.1 Explain the importance of policies, plans and procedures related to organizational security.

- **Standard operating procedure**
- **Agreement types**
  - BPA
  - SLA
  - ISA
  - MOU/MOA
- **Personnel management**
  - Mandatory vacations
  - Job rotation
  - Separation of duties
  - Clean desk
  - Background checks
  - Exit interviews
  - Role-based awareness training
    - Data owner
    - Systems administrator
    - System owner
    - User
    - Privileged user
    - Executive user
  - NDA
  - Onboarding
  - Continuing education
  - Acceptable use policy/rules of behavior
  - Adverse actions
- **General security policies**
  - Social media networks/applications
  - Personal email

5.2 Summarize business impact analysis concepts.

- **RTO/RPO**
- **MTBF**
- **MTTR**
- **Mission-essential functions**
- **Identification of critical systems**
- **Single point of failure**
- **Impact**
  - Life
  - Property
  - Safety
  - Finance
  - Reputation
- **Privacy impact assessment**
- **Privacy threshold assessment**

5.3 Explain risk management processes and concepts.

- **Threat assessment**
  - Environmental
  - Artificial/manufactured
  - Internal vs. external
- **Risk assessment**
  - SLE
  - ALE
  - ARO
  - Asset value
  - Risk register
  - Likelihood of occurrence
  - Supply chain assessment
  - Impact
  - Quantitative
  - Qualitative
  - Testing
    - Penetration testing authorization
    - Vulnerability testing authorization
  - Risk response techniques
    - Accept
    - Transfer
    - Avoid
    - Mitigate
- **Change management**

5.4 Given a scenario, follow incident response procedures.

- **Incident response plan**
  - Documented incident types/category definitions
  - Roles and responsibilities
  - Reporting requirements/escalation
  - Cyber-incident response teams
  - Exercise
- **Incident response process**
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned

5.5 Summarize basic concepts of forensics.

- **Order of volatility**
- **Chain of custody**
- **Legal hold**
- **Data acquisition**
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
  - Screenshots
  - Witness interviews
- **Preservation**
- **Recovery**
- **Strategic intelligence/ counterintelligence gathering**
  - Active logging
- **Track person hours**

5.6 Explain disaster recovery and continuity of operations concepts.

- **Recovery sites**
  - Hot site
  - Warm site
  - Cold site
- **Order of restoration**
- **Backup concepts**
  - Differential
  - Incremental
  - Snapshots
  - Full
- **Geographic considerations**
  - Off-site backups
  - Distance
  - Location selection
  - Legal implications
  - Data sovereignty
- **Continuity of operations planning**
  - Exercises/tabletop
  - After-action reports
  - Failover
  - Alternate processing sites
  - Alternate business practices

5.7 Compare and contrast various types of controls.

- **Deterrent**
- **Preventive**
- **Detective**
- **Corrective**
- **Compensating**
- **Technical**
- **Administrative**
- **Physical**

5.8 Given a scenario, carry out data security and privacy practices.

- **Data destruction and media sanitization**
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Purging
  - Wiping
- **Data sensitivity labeling and handling**
  - Confidential
  - Private
  - Public
  - Proprietary
  - PII
  - PHI
- **Data roles**
  - Owner
  - Steward/custodian
  - Privacy officer
- **Data retention**
- **Legal and compliance**

6.0 Cryptography and PKI

6.1 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**
  - Crypto service provider
  - Crypto modules
- **Perfect forward secrecy**
- **Security through obscurity**
- **Common use cases**
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality
  - Supporting integrity
  - Supporting obfuscation
  - Supporting authentication
  - Supporting non-repudiation
  - Resource vs. security constraints

6.2 Explain cryptography algorithms and their basic characteristics.

- **Symmetric algorithms**
  - AES
  - DES
  - 3DES
  - RC4
  - Blowfish/Twofish
- **Cipher modes**
  - CBC
  - GCM
  - ECB
  - CTR
  - Stream vs. block
- **Asymmetric algorithms**
  - RSA
  - DSA
  - Diffie-Hellman
    - Groups
    - DHE
    - ECDHE
  - Elliptic curve
  - PGP/GPG
- **Hashing algorithms**
  - MD5
  - SHA
  - HMAC
  - RIPEMD
- **Key stretching algorithms**
  - BCRYPT
  - PBKDF2
- **Obfuscation**
  - XOR
  - ROT13
  - Substitution ciphers

6.3 Given a scenario, install and configure wireless security settings.

- **Cryptographic protocols**
  - WPA
  - WPA2
  - CCMP
  - TKIP
- **Authentication protocols**
  - EAP
  - PEAP
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1x
  - RADIUS Federation
- **Methods**
  - PSK vs. Enterprise vs. Open
  - WPS
  - Captive portals

6.4 Given a scenario, implement public key infrastructure.

- **Components**
  - CA
  - Intermediate CA
  - CRL
  - OCSP
  - CSR
  - Certificate
  - Public key
  - Private key
  - Object identifiers (OID)
- **Concepts**
  - Online vs. offline CA
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining
- **Types of certificates**
  - Wildcard
  - SAN
  - Code signing
  - Self-signed
  - Machine/computer
  - Email
  - User
  - Root
  - Domain validation
  - Extended validation
- **Certificate formats**
  - DER
  - PEM
  - PFX
  - CER
  - P12
  - P7B

CompTIA Security+ Acronyms

The following is a list of acronyms that appear on the CompTIA Security+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
3DES	Triple Digital Encryption Standard
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-based Access Control
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
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
ASP	Application Service Provider
AUP	Acceptable Use Policy
AV	Antivirus
AV	Asset Value
BAC	Business Availability Center
BCP	Business Continuity Planning
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partners Agreement
BPDU	Bridge Protocol Data Unit
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
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CCMP	Counter-Mode/CBC-Mac Protocol
CCTV	Closed-circuit Television

ACRONYM	SPELLED OUT
CER	Certificate
CER	Cross-over Error Rate
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge Handshake Authentication Protocol
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CMS	Content Management System
COOP	Continuity of Operations Plan
COPE	Corporate Owned, Personally Enabled
CP	Contingency Planning
CRC	Cyclical Redundancy Check
CRL	Certificate Revocation List
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CSP	Cloud Service Provider
CSR	Certificate Signing Request
CSRF	Cross-site Request Forgery
CSU	Channel Service Unit
CTM	Counter-Mode
CTO	Chief Technology Officer
CTR	Counter
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DBA	Database Administrator
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DER	Distinguished Encoding Rules
DES	Digital Encryption Standard
DFIR	Digital Forensics and Investigation Response
DHCP	Dynamic Host Configuration Protocol
DHE	Data-Handling Electronics
DHE	Diffie-Hellman Ephemeral
DLL	Dynamic Link Library
DLP	Data Loss Prevention

ACRONYM	SPELLED OUT
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
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
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Exposure Factor
EFS	Encrypted File System
EMI	Electromagnetic Interference
EMP	Electro Magnetic Pulse
EOL	End of Life
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulated Security Payload
EULA	End User License Agreement
FACL	File System Access Control List
FAR	False Acceptance Rate
FDE	Full Disk Encryption
FRR	False Rejection Rate
FTP	File Transfer Protocol
FTPS	FTP over SSL
GCM	Galois Counter Mode
GPG	Gnu Privacy Guard
GPO	Group Policy Object
GPS	Global Positioning System
GPU	Graphic Processing Unit
GRE	Generic Routing Encapsulation
HA	High Availability
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/TLS
HVAC	Heating, Ventilation and Air Conditioning

ACRONYM	SPELLED OUT
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
ID	Identification
IDEA	International Data Encryption Algorithm
IDF	Intermediate Distribution Frame
IdP	Identity Provider
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IIS	Internet Information System
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP4	Internet Message Access Protocol v4
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Incident Response
IR	Infrared
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
ITCP	IT Contingency Plan
IV	Initialization Vector
KDC	Key Distribution Center
KEK	Key Encryption Key
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
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDF	Main Distribution Frame
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multi-function Device
MIME	Multipurpose Internet Mail Exchange
MMS	Multimedia Message Service
MOA	Memorandum of Agreement

ACRONYM	SPELLED OUT
MOTD	Message of the Day
MOU	Memorandum of Understanding
MPLS	Multi-Protocol Label Switching
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSP	Managed Service Provider
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Recover or Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near Field Communication
NGAC	Next Generation Access Control
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OAUTH	Open Authorization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OTA	Over The Air
OVAL	Open Vulnerability Assessment Language
P12	PKCS #12
P2P	Peer to Peer
PaaS	Platform as a Service
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
PEM	Privacy-enhanced Electronic Mail
PFS	Perfect Forward Secrecy
PFX	Personal Exchange Format
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification

ACRONYM	SPELLED OUT
PKI	Public Key Infrastructure
POODLE	Padding Oracle on Downgrade Legacy Encryption
POP	Post Office Protocol
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
RA	Registration Authority
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RAT	Remote Access Trojan
RBAC	Role-based Access Control
RBAC	Rule-based Access Control
RC4	Rivest Cipher version 4
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFID	Radio Frequency Identifier
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RMF	Risk Management Framework
RPO	Recovery Point Objective
RSA	Rivest, Shamir, & Adleman
RTBH	Remotely Triggered Black Hole
RTO	Recovery Time Objective
RTOS	Real-time Operating System
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SAN	Storage Area Network
SAN	Subject Alternative Name
SCADA	System Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy
SCSI	Small Computer System Interface
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDLM	Software Development Life Cycle Methodology
SDN	Software Defined Network
SED	Self-encrypting Drive

ACRONYM	SPELLED OUT
SEH	Structured Exception Handler
SFTP	Secured File Transfer Protocol
SHA	Secure Hashing Algorithm
SHTTP	Secure Hypertext Transfer Protocol
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIPS	Session Initiation Protocol Secure
SLA	Service Level Agreement
SLE	Single Loss Expectancy
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SoC	System on Chip
SPF	Sender Policy Framework
SPIM	Spam over Internet Messaging
SPoF	Single Point of Failure
SQL	Structured Query Language
SRTP	Secure Real-Time Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
SSP	System Security Plan
STP	Shielded Twisted Pair
TACACS+	Terminal Access Controller Access Control System Plus
TCO	Total Cost of Ownership
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
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UPS	Uninterruptable Power Supply
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USB	Universal Serial Bus
USB OTG	USB On The Go
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VDE	Virtual Desktop Environment
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Masking
VM	Virtual Machine
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
WORM	Write Once Read Many
WPA	WiFi Protected Access
WPA2	WiFi Protected Access 2
WPS	WiFi Protected Setup
WTLS	Wireless TLS
XML	Extensible Markup Language
XOR	Exclusive Or
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting

Security+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Security+ exam. This list may also be helpful for training companies that wish to create a lab component to their training offering. The bulleted lists below each topic are sample lists and not exhaustive.

EQUIPMENT

- Router
- Firewall
- Access point
- Switch
- IDS/IPS
- Server
- Content filter
- Client
- Mobile device
- VPN concentrator
- UTM
- Enterprise security managers/SIEM suite
- Load balancer
- Proxies
- DLP appliance
- ICS or similar systems
- Network access control servers
- DDoS mitigation hardware

SPARE PARTS/HARDWARE

- Keyboards
- Mice
- Network cables
- Monitors
- Wireless and Bluetooth dongles

HARDWARE TOOLS

- WiFi analyzers
- Hardware debuggers

SOFTWARE TOOLS AND SOFTWARE TOOLS

- Exploitation distributions (e.g., Kali)
- Proxy server
- Virtualization software
- Virtualized appliances
- Wireshark
- tcpdump
- NMAP
- OpenVAS
- Metasploit/Metaspoitable2
- Back Orifice
- Cain & Abel
- John the Ripper
- pfSense
- Security Onion
- Roo
- Any UTM

OTHER

- SourceForge

CompTIA