



# CompTIA Security+ Certification Exam Objectives

**EXAM NUMBER: SY0-501**



# About the Exam

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 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; and 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](mailto: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	CompTIA Security+ 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%
<b>Total</b>	<b>100%</b>



# 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
  - Man-in-the-middle
  - Buffer overflow
- Injection
- Cross-site scripting
- Cross-site request forgery
- Privilege escalation
- ARP poisoning
- Amplification
- DNS poisoning
- Domain hijacking
- Man-in-the-browser
- 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**
  - **Black box**
  - **White box**
  - **Gray box**
  - **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
- tracer
- nslookup/dig
- arp
- ipconfig/ip/ifconfig
- tcpdump
- nmap
- netcat



### 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 whitelisting
- 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
  - Sideloaded
  - 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**
  - DMZ
  - 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 whitelisting/blacklisting
- Disable default accounts/passwords
- **Peripherals**
  - Wireless keyboards
  - Wireless mice
  - Displays
  - WiFi-enabled MicroSD cards
  - Printers/MFDs
  - External storage devices
  - Digital cameras





### 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**
- **Mantrap**
- **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)
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Multifactor authentication
  - Something you are
- 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



## 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
  - System 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
  - Manmade
  - 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
- **Incident response process**
  - Preparation
  - Identification
- **Cyber-incident response teams**
  - Exercise
- **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 man-hours**

#### 5.6 Explain disaster recovery and continuity of operation 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 operation 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 a part of a comprehensive exam preparation program.

<b>ACRONYM</b>	<b>SPELLED OUT</b>	<b>ACRONYM</b>	<b>SPELLED OUT</b>
3DES	Triple Digital Encryption Standard	CER	Cross-over Error Rate
AAA	Authentication, Authorization, and Accounting	CERT	Computer Emergency Response Team
ABAC	Attribute-based Access Control	CFB	Cipher Feedback
ACL	Access Control List	CHAP	Challenge Handshake Authentication Protocol
AES	Advanced Encryption Standard	CIO	Chief Information Officer
AES256	Advanced Encryption Standards 256bit	CIRT	Computer Incident Response Team
AH	Authentication Header	CMS	Content Management System
ALE	Annualized Loss Expectancy	COOP	Continuity of Operations Plan
AP	Access Point	COPE	Corporate Owned, Personally Enabled
API	Application Programming Interface	CP	Contingency Planning
APT	Advanced Persistent Threat	CRC	Cyclical Redundancy Check
ARO	Annualized Rate of Occurrence	CRL	Certificate Revocation List
ARP	Address Resolution Protocol	CSIRT	Computer Security Incident Response Team
ASLR	Address Space Layout Randomization	CSO	Chief Security Officer
ASP	Application Service Provider	CSP	Cloud Service Provider
AUP	Acceptable Use Policy	CSR	Certificate Signing Request
AV	Antivirus	CSRF	Cross-site Request Forgery
AV	Asset Value	CSU	Channel Service Unit
BAC	Business Availability Center	CTM	Counter-Mode
BCP	Business Continuity Planning	CTO	Chief Technology Officer
BIA	Business Impact Analysis	CTR	Counter
BIOS	Basic Input/Output System	CYOD	Choose Your Own Device
BPA	Business Partners Agreement	DAC	Discretionary Access Control
BPDU	Bridge Protocol Data Unit	DBA	Database Administrator
BYOD	Bring Your Own Device	DDoS	Distributed Denial of Service
CA	Certificate Authority	DEP	Data Execution Prevention
CAC	Common Access Card	DER	Distinguished Encoding Rules
CAN	Controller Area Network	DES	Digital Encryption Standard
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart	DFIR	Digital Forensics and Investigation Response
CAR	Corrective Action Report	DHCP	Dynamic Host Configuration Protocol
CBC	Cipher Block Chaining	DHE	Data-Handling Electronics
CCMP	Counter-Mode/CBC-Mac Protocol	DHE	Diffie-Hellman Ephemeral
CCTV	Closed-circuit Television	DLL	Dynamic Link Library
CER	Certificate	DLP	Data Loss Prevention
		DMZ	Demilitarized Zone



DNAT	Destination Network Address Transaction	IDEA	International Data Encryption Algorithm
DNS	Domain Name Service (Server)	IDF	Intermediate Distribution Frame
DoS	Denial of Service	IdP	Identity Provider
DRP	Disaster Recovery Plan	IDS	Intrusion Detection System
DSA	Digital Signature Algorithm	IEEE	Institute of Electrical and Electronic Engineers
DSL	Digital Subscriber Line	IIS	Internet Information System
DSU	Data Service Unit	IKE	Internet Key Exchange
EAP	Extensible Authentication Protocol	IM	Instant Messaging
ECB	Electronic Code Book	IMAP4	Internet Message Access Protocol v4
ECC	Elliptic Curve Cryptography	IoT	Internet of Things
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral	IP	Internet Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm	IPSec	Internet Protocol Security
EFS	Encrypted File System	IR	Incident Response
EMI	Electromagnetic Interference	IR	Infrared
EMP	Electro Magnetic Pulse	IRC	Internet Relay Chat
ERP	Enterprise Resource Planning	IRP	Incident Response Plan
ESN	Electronic Serial Number	ISA	Interconnection Security Agreement
ESP	Encapsulated Security Payload	ISP	Internet Service Provider
EF	Exposure Factor	ISSO	Information Systems Security Officer
FACL	File System Access Control List	ITCP	IT Contingency Plan
FAR	False Acceptance Rate	IV	Initialization Vector
FDE	Full Disk Encryption	KDC	Key Distribution Center
FRR	False Rejection Rate	KEK	Key Encryption Key
FTP	File Transfer Protocol	L2TP	Layer 2 Tunneling Protocol
FTPS	Secured File Transfer Protocol	LAN	Local Area Network
GCM	Galois Counter Mode	LDAP	Lightweight Directory Access Protocol
GPG	Gnu Privacy Guard	LEAP	Lightweight Extensible Authentication Protocol
GPO	Group Policy Object	MaaS	Monitoring as a Service
GPS	Global Positioning System	MAC	Mandatory Access Control
GPU	Graphic Processing Unit	MAC	Media Access Control
GRE	Generic Routing Encapsulation	MAC	Message Authentication Code
HA	High Availability	MAN	Metropolitan Area Network
HDD	Hard Disk Drive	MBR	Master Boot Record
HIDS	Host-based Intrusion Detection System	MD5	Message Digest 5
HIPS	Host-based Intrusion Prevention System	MDF	Main Distribution Frame
HMAC	Hashed Message Authentication Code	MDM	Mobile Device Management
HOTP	HMAC-based One-Time Password	MFA	Multi-Factor Authentication
HSM	Hardware Security Module	MFD	Multi-function Device
HTML	Hypertext Markup Language	MITM	Man-in-the-Middle
HTTP	Hypertext Transfer Protocol	MMS	Multimedia Message Service
HTTPS	Hypertext Transfer Protocol over SSL/TLS	MOA	Memorandum of Agreement
HVAC	Heating, Ventilation and Air Conditioning	MOU	Memorandum of Understanding
IaaS	Infrastructure as a Service	MPLS	Multi-protocol Label Switching
ICMP	Internet Control Message Protocol	MSCHAP	Microsoft Challenge Handshake Authentication Protocol
ICS	Industrial Control Systems		
ID	Identification	MSP	Managed Service Provider

<b>ACRONYM</b>	<b>SPELLED OUT</b>	<b>ACRONYM</b>	<b>SPELLED OUT</b>
MTBF	Mean Time Between Failures	PSK	Pre-shared Key
MTTF	Mean Time to Failure	PTZ	Pan-Tilt-Zoom
MTTR	Mean Time to Recover or Mean Time to Repair	RA	Recovery Agent
MTU	Maximum Transmission Unit	RA	Registration Authority
NAC	Network Access Control	RAD	Rapid Application Development
NAT	Network Address Translation	RADIUS	Remote Authentication Dial-in User Server
NDA	Non-disclosure Agreement	RAID	Redundant Array of Inexpensive Disks
NFC	Near Field Communication	RAS	Remote Access Server
NGAC	Next Generation Access Control	RAT	Remote Access Trojan
NIDS	Network-based Intrusion Detection System	RBAC	Role-based Access Control
NIPS	Network-based Intrusion Prevention System	RBAC	Rule-based Access Control
NIST	National Institute of Standards & Technology	RC4	Rivest Cipher version 4
NTFS	New Technology File System	RDP	Remote Desktop Protocol
NTLM	New Technology LAN Manager	RFID	Radio Frequency Identifier
NTP	Network Time Protocol	RIPEMD	RACE Integrity Primitives Evaluation Message Digest
OAUTH	Open Authorization	ROI	Return on Investment
OCSP	Online Certificate Status Protocol	RMF	Risk Management Framework
OID	Object Identifier	RPO	Recovery Point Objective
OS	Operating System	RSA	Rivest, Shamir, & Adleman
OTA	Over The Air	RTBH	Remotely Triggered Black Hole
OVAL	Open Vulnerability Assessment Language	RTO	Recovery Time Objective
P12	PKCS #12	RTOS	Real-time Operating System
P2P	Peer to Peer	RTP	Real-time Transport Protocol
PaaS	Platform as a Service	S/MIME	Secure/Multipurpose Internet Mail Extensions
PAC	Proxy Auto Configuration	SaaS	Software as a Service
PAM	Pluggable Authentication Modules	SAML	Security Assertions Markup Language
PAP	Password Authentication Protocol	SAN	Storage Area Network
PAT	Port Address Translation	SAN	Subject Alternative Name
PBKDF2	Password-based Key Derivation Function 2	SCADA	System Control and Data Acquisition
PBX	Private Branch Exchange	SCAP	Security Content Automation Protocol
PCAP	Packet Capture	SCEP	Simple Certificate Enrollment Protocol
PEAP	Protected Extensible Authentication Protocol	SCP	Secure Copy
PED	Personal Electronic Device	SCSI	Small Computer System Interface
PEM	Privacy-enhanced Electronic Mail	SDK	Software Development Kit
PFS	Perfect Forward Secrecy	SDLC	Software Development Life Cycle
PFX	Personal Exchange Format	SDLM	Software Development Life Cycle Methodology
PGP	Pretty Good Privacy	SDN	Software Defined Network
PHI	Personal Health Information	SED	Self-encrypting Drive
PII	Personally Identifiable Information	SEH	Structured Exception Handler
PIV	Personal Identity Verification	SFTP	Secured File Transfer Protocol
PKI	Public Key Infrastructure	SHA	Secure Hashing Algorithm
POODLE	Padding Oracle on Downgrade Legacy Encryption	SHTTP	Secure Hypertext Transfer Protocol
POP	Post Office Protocol	SIEM	Security Information and Event Management
POTS	Plain Old Telephone Service	SIM	Subscriber Identity Module
PPP	Point-to-Point Protocol	SLA	Service Level Agreement
PPTP	Point-to-Point Tunneling Protocol		

<b>ACRONYM</b>	<b>SPELLED OUT</b>
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
STP	Shielded Twisted Pair
TACACS+	Terminal Access Controller Access Control System Plus
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
UAV	Unmanned Aerial Vehicle
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

<b>ACRONYM</b>	<b>SPELLED OUT</b>
VTC	Video Conferencing
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 who wish to create a lab component to their training offering. The bulleted lists below each topic are a sample list 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/Metasploitable2
- Back Orifice
- Cain & Abel
- John the Ripper
- pfSense
- Security Onion
- Roo
- Any UTM

## **OTHER**

- SourceForge