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:

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Threats, Attacks and Vulnerabilities</td>
<td>21%</td>
</tr>
<tr>
<td>2.0 Technologies and Tools</td>
<td>22%</td>
</tr>
<tr>
<td>3.0 Architecture and Design</td>
<td>15%</td>
</tr>
<tr>
<td>4.0 Identity and Access Management</td>
<td>16%</td>
</tr>
<tr>
<td>5.0 Risk Management</td>
<td>14%</td>
</tr>
<tr>
<td>6.0 Cryptography and PKI</td>
<td>12%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
### 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
- **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 Security+ Certification Exam Objectives Version 4.0 (Exam Number: SY0-501)
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
  - Sidelading
  - 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
  - LDAP
  - 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
- SDN
- Proxies
- Firewalls
- VPN concentrators
- SSL accelerators
- Load balancers
- DDoS mitigator
- Aggregation switches
- Taps and port mirror

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)
- 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
- Account policy enforcement
  - Credential management
- 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
- 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
    - 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
  - 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
5.0 Risk 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 man-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
  - AES
  - DES
  - 3DES
  - RC4
  - Blowfish/Twofish
- Modes of operation
- Asymmetric algorithms
  - RSA
  - DSA
  - Diffie-Hellman
  - Groups
  - DHE
  - ECDHE
- Hashing algorithms
  - MD5
  - SHA
- 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
- Key stretching algorithms
  - HMAC
  - RIPEMD
- Obfuscation
  - XOR
  - ROT13
  - Substitution ciphers
6.0 Cryptography and PKI

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

- **Methods**
  - IEEE 802.1x
  - RADIUS Federation

- **Components**
  - CA
  - Intermediate CA
  - CRL
  - OCSP
  - CSR
  - Certificate
  - Public key
  - Private key
  - Object identifiers (OID)

- **Concepts**
  - Online vs. offline CA

6.4 Given a scenario, implement public key infrastructure.

- **Components**
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining

- **Types of certificates**
  - Wildcard
  - SAN
  - Code signing
  - Self-signed
  - Machine/computer
  - Email

- **Methods**
  - PSK vs. Enterprise vs. Open
  - WPS
  - Captive portals

- **Certificate formats**
  - DER
  - PEM
  - PFX
  - CER
  - P12
  - P7B
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.
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>DNAT</td>
<td>Destination Network Address Transaction</td>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service (Server)</td>
<td>ICS</td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
<td>IDEA</td>
<td>International Data Encryption Algorithm</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
<td>IDP</td>
<td>Identity Provider</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>DSU</td>
<td>Data Service Unit</td>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
<td>IIS</td>
<td>Internet Information System</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Code Book</td>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>ECDHE</td>
<td>Elliptic Curve Diffie-Hellman Ephemeral</td>
<td>IMAP4</td>
<td>Internet Message Access Protocol v4</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic Curve Digital Signature Algorithm</td>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>EF</td>
<td>Exposure Factor</td>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>EFS</td>
<td>Encrypted File System</td>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
<td>IR</td>
<td>Incident Response</td>
</tr>
<tr>
<td>EMP</td>
<td>Electro Magnetic Pulse</td>
<td>IR</td>
<td>Infrared</td>
</tr>
<tr>
<td>EOL</td>
<td>End of Life</td>
<td>IRC</td>
<td>Internet Relay Chat</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
<td>IRP</td>
<td>Incident Response Plan</td>
</tr>
<tr>
<td>ESN</td>
<td>Electronic Serial Number</td>
<td>ISA</td>
<td>Interconnection Security Agreement</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulated Security Payload</td>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>EULA</td>
<td>End User License Agreement</td>
<td>ISSO</td>
<td>Information Systems Security Officer</td>
</tr>
<tr>
<td>FACL</td>
<td>File System Access Control List</td>
<td>ITCP</td>
<td>IT Contingency Plan</td>
</tr>
<tr>
<td>FAR</td>
<td>False Acceptance Rate</td>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>FDE</td>
<td>Full Disk Encryption</td>
<td>KDC</td>
<td>Key Distribution Center</td>
</tr>
<tr>
<td>FRR</td>
<td>False Rejection Rate</td>
<td>KEK</td>
<td>Key Encryption Key</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>FTPS</td>
<td>Secure File Transfer Protocol</td>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>GCM</td>
<td>Galois Counter Mode</td>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>GPG</td>
<td>Gnu Privacy Guard</td>
<td>LEAP</td>
<td>Lightweight Extensible Authentication Protocol</td>
</tr>
<tr>
<td>GPO</td>
<td>Group Policy Object</td>
<td>MaaS</td>
<td>Monitoring as a Service</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
<td>MAC</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphic Processing Unit</td>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
<td>MBR</td>
<td>Master Boot Record</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host-based Intrusion Detection System</td>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>HIPS</td>
<td>Host-based Intrusion Prevention System</td>
<td>MDF</td>
<td>Main Distribution Frame</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hashed Message Authentication Code</td>
<td>MDM</td>
<td>Mobile Device Management</td>
</tr>
<tr>
<td>HOTP</td>
<td>HMAC-based One-Time Password</td>
<td>MFA</td>
<td>Multifactor Authentication</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
<td>MFD</td>
<td>Multi-function Device</td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language</td>
<td>MIME</td>
<td>Multipurpose Internet Mail Exchange</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td>MITM</td>
<td>Man-in-the-Middle</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol over SSL/TLS</td>
<td>MMS</td>
<td>Multimedia Message Service</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation and Air Conditioning</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CompTIA Security+ Certification Exam Objectives Version 4.0 (Exam Number: SY0-501)
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOA</td>
<td>Memorandum of Agreement</td>
</tr>
<tr>
<td>MOTD</td>
<td>Message of the Day</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi-Protocol Label Switching</td>
</tr>
<tr>
<td>MSCHAP</td>
<td>Microsoft Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>MSP</td>
<td>Managed Service Provider</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time to Failure</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time to Recover or Mean Time to Repair</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NDA</td>
<td>Non-disclosure Agreement</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>NGAC</td>
<td>Next Generation Access Control</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network-based Intrusion Detection System</td>
</tr>
<tr>
<td>NIPS</td>
<td>Network-based Intrusion Prevention System</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards &amp; Technology</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>NTLM</td>
<td>New Technology LAN Manager</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OAUTH</td>
<td>Open Authorization</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OTA</td>
<td>Over The Air</td>
</tr>
<tr>
<td>OVAL</td>
<td>Open Vulnerability Assessment Language</td>
</tr>
<tr>
<td>P12</td>
<td>PKCS #12</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer to Peer</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PAC</td>
<td>Proxy Auto Configuration</td>
</tr>
<tr>
<td>PAM</td>
<td>Pluggable Authentication Modules</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PBKDF2</td>
<td>Password-based Key Derivation Function 2</td>
</tr>
<tr>
<td>PBX</td>
<td>Private Branch Exchange</td>
</tr>
<tr>
<td>PCAP</td>
<td>Packet Capture</td>
</tr>
<tr>
<td>PEAEP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>PED</td>
<td>Personal Electronic Device</td>
</tr>
<tr>
<td>PEM</td>
<td>Privacy-enhanced Electronic Mail</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PFX</td>
<td>Personal Exchange Format</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>POODLE</td>
<td>Padding Oracle on Downgrade Legacy Encryption</td>
</tr>
<tr>
<td>POP</td>
<td>Post Office Protocol</td>
</tr>
<tr>
<td>POTS</td>
<td>Plain Old Telephone Service</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-shared Key</td>
</tr>
<tr>
<td>PTZ</td>
<td>Pan-Tilt-Zoom</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>RA</td>
<td>Recovery Agent</td>
</tr>
<tr>
<td>RAD</td>
<td>Rapid Application Development</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-in User Server</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Inexpensive Disks</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Server</td>
</tr>
<tr>
<td>RAT</td>
<td>Remote Access Trojan</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-based Access Control</td>
</tr>
<tr>
<td>RBAC</td>
<td>Rule-based Access Control</td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher version 4</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identifier</td>
</tr>
<tr>
<td>RIPEMD</td>
<td>RACE Integrity Primitives</td>
</tr>
<tr>
<td>ROI</td>
<td>Return on Investment</td>
</tr>
<tr>
<td>RMF</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, &amp; Adleman</td>
</tr>
<tr>
<td>RTBH</td>
<td>Remotely Triggered Black Hole</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>RTOS</td>
<td>Real-time Operating System</td>
</tr>
<tr>
<td>RTP</td>
<td>Real-time Transport Protocol</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure/Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertions Markup Language</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SAN</td>
<td>Subject Alternative Name</td>
</tr>
<tr>
<td>SCADA</td>
<td>System Control and Data Acquisition</td>
</tr>
<tr>
<td>SCAP</td>
<td>Security Content Automation Protocol</td>
</tr>
<tr>
<td>SCEP</td>
<td>Simple Certificate Enrollment Protocol</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy</td>
</tr>
<tr>
<td>SCSI</td>
<td>Small Computer System Interface</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>SDLM</td>
<td>Software Development Life Cycle Methodology</td>
</tr>
<tr>
<td>SDN</td>
<td>Software Defined Network</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>SED</td>
<td>Self-encrypting Drive</td>
</tr>
<tr>
<td>SEH</td>
<td>Structured Exception Handler</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secured File Transfer Protocol</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
</tr>
<tr>
<td>SHTTP</td>
<td>Secure Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SIPS</td>
<td>Session Initiation Protocol Secure</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SLE</td>
<td>Single Loss Expectancy</td>
</tr>
<tr>
<td>SMB</td>
<td>Server Message Block</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SMTPS</td>
<td>Simple Mail Transfer Protocol Secure</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SoC</td>
<td>System on Chip</td>
</tr>
<tr>
<td>SPF</td>
<td>Sender Policy Framework</td>
</tr>
<tr>
<td>SPIM</td>
<td>Spam over Internet Messaging</td>
</tr>
<tr>
<td>SPoF</td>
<td>Single Point of Failure</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SRTP</td>
<td>Secure Real-Time Protocol</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-on</td>
</tr>
<tr>
<td>SSP</td>
<td>System Security Plan</td>
</tr>
<tr>
<td>STP</td>
<td>Shielded Twisted Pair</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System Plus</td>
</tr>
<tr>
<td>TCO</td>
<td>Total Cost of Ownership</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TGT</td>
<td>Ticket Granting Ticket</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TOTP</td>
<td>Time-based One-time Password</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>TSIG</td>
<td>Transaction Signature</td>
</tr>
<tr>
<td>UAT</td>
<td>User Acceptance Testing</td>
</tr>
<tr>
<td>UAV</td>
<td>Unmanned Aerial Vehicle</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>URI</td>
<td>Uniform Resource Identifier</td>
</tr>
</tbody>
</table>
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

**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

**SPARE PARTS/HARDWARE**
- Keyboards
- Mice
- Network cables
- Monitors
- Wireless and Bluetooth dongles

**OTHER**
- SourceForge