CompTIA Security+ Certification Exam Objectives

EXAM NUMBER: SY0-401
About the Exam

The CompTIA Security+ certification is a vendor-neutral, internationally recognized credential used by organizations and security professionals around the globe to validate foundation-level security skills and knowledge. Candidates are encouraged to use this document to help prepare for CompTIA Security+ SY0-401, which measures necessary skills for IT security professionals. Successful candidates will have the knowledge required to:

- Identify risk
- Participate in risk mitigation activities
- Provide infrastructure, application, information and operational security
- Apply security controls to maintain confidentiality, integrity and availability
- Identify appropriate technologies and products
- Troubleshoot security events and incidents
- Operate with an awareness of applicable policies, laws and regulations

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 perform a search using CertGuard’s engine, found here.

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+ SY0-401
- 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 Network Security</td>
<td>20%</td>
</tr>
<tr>
<td>2.0 Compliance and Operational Security</td>
<td>18%</td>
</tr>
<tr>
<td>3.0 Threats and Vulnerabilities</td>
<td>20%</td>
</tr>
<tr>
<td>4.0 Application, Data and Host Security</td>
<td>15%</td>
</tr>
<tr>
<td>5.0 Access Control and Identity Management</td>
<td>15%</td>
</tr>
<tr>
<td>6.0 Cryptography</td>
<td>12%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
1.0 Network Security

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

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

1.2 Given a scenario, use secure network administration principles.

- Rule-based management
- Firewall rules
- VLAN management
- Secure router configuration
- Access control lists
- Port security
  - 802.1x
- Flood guards
- Loop protection
- Implicit deny
- Network separation
- Log analysis
- Unified threat management

1.3 Explain network design elements and components.

- DMZ
- Subnetting
- VLAN
- NAT
- Remote access
- Telephony
- NAC
- Virtualization
- Cloud computing  
  - PaaS
  - SaaS
  - IaaS
  - Private
  - Public
  - Hybrid
  - Community
- Layered security/defense in depth
### 1.4 Given a scenario, implement common protocols and services.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>21</td>
</tr>
<tr>
<td>IPv6</td>
<td>22</td>
</tr>
<tr>
<td>iSCSI</td>
<td>25</td>
</tr>
<tr>
<td>Fibre Channel</td>
<td>53</td>
</tr>
<tr>
<td>FCoE</td>
<td>80</td>
</tr>
<tr>
<td>FTP</td>
<td>110</td>
</tr>
<tr>
<td>SFTP</td>
<td>139</td>
</tr>
<tr>
<td>TFTP</td>
<td>143</td>
</tr>
<tr>
<td>TELNET</td>
<td>443</td>
</tr>
<tr>
<td>HTTP</td>
<td>3389</td>
</tr>
<tr>
<td>NetBIOS</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>WPA</th>
<th>MAC filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2</td>
<td>Disable SSID broadcast</td>
</tr>
<tr>
<td>WEP</td>
<td>TKIP</td>
</tr>
<tr>
<td>EAP</td>
<td>CCMP</td>
</tr>
<tr>
<td>PEAP</td>
<td>Antenna placement</td>
</tr>
<tr>
<td>LEAP</td>
<td>Power level controls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WPA</th>
<th>Captive portals</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2</td>
<td>Antenna types</td>
</tr>
<tr>
<td>WEP</td>
<td>Site surveys</td>
</tr>
<tr>
<td>EAP</td>
<td>VPN (over open wireless)</td>
</tr>
</tbody>
</table>
2.0 Compliance and Operational Security

2.1 Explain the importance of risk related concepts.

- **Control types**
  - Technical
  - Management
  - Operational
- **False positives**
- **False negatives**
- **Importance of policies in reducing risk**
  - Privacy policy
  - Acceptable use
  - Security policy
  - Mandatory vacations
  - Job rotation
  - Separation of duties
  - Least privilege
- **Risk calculation**
  - Likelihood
  - ALE
  - Impact
  - SLE
  - ARO
  - MTTR
  - MTTF
  - MTBF
- **Quantitative vs. qualitative**
- **Vulnerabilities**
- **Threat vectors**
- **Probability/threat likelihood**
- **Risk avoidance, transference, acceptance, mitigation, deterrence**
- **Risks associated with cloud computing and virtualization**
- **Recovery time objective and recovery point objective**

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

- **On-boarding/off-boarding business partners**
- **Social media networks and/or applications**
- **Interoperability agreements**
  - SLA
  - BPA
  - MOU
  - ISA
- **Privacy considerations**
- **Risk awareness**
- **Unauthorized data sharing**
- **Data ownership**
- **Data backups**
- **Follow security policy and procedures**
- **Review agreement requirements to verify compliance and performance standards**

2.3 Given a scenario, implement appropriate risk mitigation strategies.

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

2.4 Given a scenario, implement basic forensic procedures.
- Order of volatility
- Capture system image
- Network traffic and logs
- Capture video
- Record time offset
- Take hashes
- Screenshots
- Witnesses
- Track man hours and expense
- Chain of custody
- Big Data analysis

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

2.6 Explain the importance of security related awareness and training.
- Security policy training and procedures
- Role-based training
- Personally identifiable information
- Information classification
  - High
  - Medium
  - Low
  - Confidential
  - Private
  - Public
- Data labeling, handling and disposal
- Compliance with laws, best practices and standards
- User habits
  - Password behaviors
  - Data handling
  - Clean desk policies
  - Prevent tailgating
  - Personally owned devices
- New threats and new security trends/alerts
  - New viruses
  - Phishing attacks
  - Zero-day exploits
- Use of social networking and P2P
  - Follow up and gather training metrics to validate compliance and security posture

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

CompTIA Security+ Certification Exam Objectives Version 1.0 (Exam Number: SY0-401)
Summarize risk management best practices.

2.8 Business continuity concepts
- Business impact analysis
- Identification of critical systems and components
- Removing single points of failure
- Business continuity planning and testing
- Risk assessment
- Continuity of operations
- Disaster recovery
- IT contingency planning
- Succession planning
- High availability
- Redundancy
- Tabletop exercises

2.9 Fault tolerance
- Hardware
- RAID
- Clustering
- Load balancing
- Servers

Disaster recovery concepts
- Backup plans/policies
- Backup execution/frequency
- Cold site
- Hot site
- Warm site

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

2.8 Confidentiality
- Encryption
- Access controls
- Steganography

Integrity
- Hashing
- Digital signatures
- Certificates
- Non-repudiation

2.9 Availability
- Redundancy
- Fault tolerance
- Patching

Safety
- Fencing
- Lighting
- Locks
- CCTV

- Escape plans
- Drills
- Escape routes
- Testing controls
# 3.0 Threats and Vulnerabilities

## 3.1 Explain types of malware.

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

## 3.2 Summarize various types of attacks.

- Man-in-the-middle
- DDoS
- DoS
- Replay
- Smurf attack
- Spoofing
- Spam
- Phishing
- Spim
- Vishing
- Spear phishing
- Xmas attack
- Pharming
- Privilege escalation
- Malicious insider threat
- DNS poisoning and ARP poisoning
- Transitive access
- Client-side attacks
- Password attacks
  - Brute force
  - Dictionary attacks
  - Hybrid
  - Birthday attacks
  - Rainbow tables
  - Typo squatting/URL hijacking
  - Watering hole attack

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

- Shoulder surfing
- Dumpster diving
- Tailgating
- Impersonation
- Hoaxes
- Whaling
- Vishing
- Principles (reasons for effectiveness)
  - Authority
  - Intimidation
- Consensus/social proof
  - Scarcity
  - Urgency
  - Familiarity/liking
  - Trust

## 3.4 Explain types of wireless attacks.

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

3.5 Explain types of application attacks.
- Cross-site scripting
- SQL injection
- LDAP injection
- XML injection
- Directory traversal/command injection
- Buffer overflow
- Integer overflow
- Zero-day
- Cookies and attachments
- Locally Shared Objects (LSOs)
- Flash cookies
- Malicious add-ons
- Session hijacking
- Header manipulation
- Arbitrary code execution/remote code execution

3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.
- Monitoring system logs
  - Event logs
  - Audit logs
  - Security logs
  - Access logs
- Network security
  - MAC limiting and filtering
  - 802.1x
  - Disabling unused interfaces and unused application service ports
  - Rogue machine detection
- Hardening
  - Disabling unnecessary services
  - Protecting management interfaces and applications
  - Password protection
  - Disabling unnecessary accounts
- Security posture
  - Initial baseline configuration
  - Continuous security monitoring
  - Remediation
- Reporting
  - Alarms
  - Alerts
  - Trends
- Detection controls vs. prevention controls
  - IDS vs. IPS
  - Camera vs. guard

3.7 Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.
- Interpret results of security assessment tools
- Tools
  - Protocol analyzer
  - Vulnerability scanner
  - Honeypots
  - Honeynets
  - Port scanner
- Passive vs. active tools
- Banner grabbing
- Risk calculations
- Threat vs. likelihood
- Assessment types
  - Risk
  - Threat
  - Vulnerability
- Assessment technique
  - Baseline reporting
  - Code review
  - Determine attack surface
  - Review architecture
  - Review designs

3.8 Explain the proper use of penetration testing versus vulnerability scanning.
- Penetration testing
  - Verify a threat exists
  - Bypass security controls
  - Actively test security controls
  - Exploiting vulnerabilities
- Vulnerability scanning
  - Passively testing security controls
  - Identify vulnerability
  - Identify lack of security controls
  - Identify common misconfigurations
  - Intrusive vs. non-intrusive
- Credentialed vs. non-credentialed
- False positive
- Black box
- White box
- Gray box
4.0 Application, Data and Host Security

4.1 Explain the importance of application security controls and techniques.

- Fuzzing
- Secure coding concepts
  - Error and exception handling
  - Input validation
- Cross-site scripting prevention
- Cross-site Request Forgery (XSRF) prevention
- Application configuration baseline (proper settings)
- Application hardening
- Application patch management
- NoSQL databases vs. SQL databases
- Server-side vs. client-side validation

4.2 Summarize mobile security concepts and technologies.

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

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

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

CompTIA Security+ Certification Exam Objectives Version 1.0 (Exam Number: SY0-401)
4.4 Implement the appropriate controls to ensure data security.

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

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

- Environments
  - SCADA
  - Embedded (printer, smart TV, HVAC control)
  - Android
  - iOS
  - Mainframe
  - Game consoles
  - In-vehicle computing systems
- Methods
  - Network segmentation
  - Security layers
  - Application firewalls
  - Manual updates
  - Firmware version control
  - Wrappers
  - Control redundancy and diversity
5.0 Access Control and Identity Management

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

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

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

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

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

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

CompTIA Security+ Certification Exam Objectives Version 1.0 (Exam Number: SY0-401)
6.0 Cryptography

6.1 Given a scenario, utilize general cryptography concepts.

- Symmetric vs. asymmetric
- Session keys
- In-band vs. out-of-band key exchange
- Fundamental differences and encryption methods
  - Block vs. stream
- Transport encryption
- Non-repudiation
- Hashing
- Key escrow
- Steganography
- Digital signatures
- Use of proven technologies
- Elliptic curve and quantum cryptography
- Ephemeral key
- Perfect forward secrecy

6.2 Given a scenario, use appropriate cryptographic methods.

- WEP vs. WPA/WPA2 and pre-shared key
- MD5
- SHA
- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA
- Diffie-Hellman
- RC4
- One-time pads
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- Twofish
- DHE
- ECDHE
- CHAP
- PAP
- Comparative strengths and performance of algorithms
- Use of algorithms/protocols with transport encryption
  - SSL
  - TLS
  - IPSec
  - SSH
  - HTTPS
- Cipher suites
  - Strong vs. weak ciphers
- Key stretching
  - PBKDF2
  - Bcrypt

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

- Certificate authorities and digital certificates
  - CA
  - CRLs
  - OCSP
  - CSR
- PKI
- Recovery agent
- Public key
- Private key
- Registration
- Key escrow
- Trust models
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.

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>Triple Digital Encryption Standard</td>
<td>CP</td>
<td>Contingency Planning</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
<td>CRC</td>
<td>Cyclical Redundancy Check</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>AES256</td>
<td>Advanced Encryption Standards 256-bit</td>
<td>CSR</td>
<td>Certificate Signing Request</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
<td>CSRF</td>
<td>Cross-Site Request Forgery</td>
</tr>
<tr>
<td>ALE</td>
<td>Annualized Loss Expectancy</td>
<td>CSU</td>
<td>Channel Service Unit</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td>CTO</td>
<td>Chief Technology Officer</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>ASP</td>
<td>Application Service Provider</td>
<td>DBA</td>
<td>Database Administrator</td>
</tr>
<tr>
<td>ARO</td>
<td>Annualized Rate of Occurrence</td>
<td>DDOS</td>
<td>Distributed Denial Of Service</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
<td>DEP</td>
<td>Data Execution Prevention</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
<td>DES</td>
<td>Digital Encryption Standard</td>
</tr>
<tr>
<td>BAC</td>
<td>Business Availability Center</td>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Planning</td>
<td>DHE</td>
<td>Data-Handling Electronics</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
<td>DHE</td>
<td>Diffie-Hellman Ephemeral</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
<td>DLL</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>BPA</td>
<td>Business Partners Agreement</td>
<td>DLP</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
<td>DNAT</td>
<td>Destination Network Address Transaction</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
<td>DNS</td>
<td>Domain Name Service (Server)</td>
</tr>
<tr>
<td>CAC</td>
<td>Common Access Card</td>
<td>DOS</td>
<td>Denial Of Service</td>
</tr>
<tr>
<td>CAN</td>
<td>Controller Area Network</td>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>Completely Automated Public Turing test to tell Computers and Humans Apart</td>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>CAR</td>
<td>Corrective Action Report</td>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>CCMP</td>
<td>Counter-mode/CBC-MAC Protocol</td>
<td>DSU</td>
<td>Data Service Unit</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>CFB</td>
<td>Cipher Feedback</td>
<td>ECDHE</td>
<td>Elliptic Curve Diffie-Hellman Exchange</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
<td>ECDSA</td>
<td>Elliptic Curve Digital Signature Algorithm</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
<td>EFS</td>
<td>Encrypted File System</td>
</tr>
<tr>
<td>CIRT</td>
<td>Computer Incident Response Team</td>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>CMS</td>
<td>Content Management System</td>
<td>ESN</td>
<td>Electronic Serial Number</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity Of Operation Planning</td>
<td>ESP</td>
<td>Encapsulated Security Payload</td>
</tr>
<tr>
<td>FACIL</td>
<td>File system Access Control List</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDE</td>
<td>Full Disk Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTPS</td>
<td>Secured File Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GCM</td>
<td>Galois Counter Mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPG</td>
<td>GNU Privacy Guard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPO</td>
<td>Group Policy Object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPU</td>
<td>Graphic Processing Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIDS</td>
<td>Host-based Intrusion Detection System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPS</td>
<td>Host-based Intrusion Prevention System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMAC</td>
<td>Hashed Message Authentication Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOTP</td>
<td>HMAC-based One Time Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol over SSL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation and Air Conditioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDF</td>
<td>Intermediate Distribution Frame</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IdP</td>
<td>Identity Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP4</td>
<td>Internet Message Access Protocol v4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRP</td>
<td>Incident Response Procedure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISA</td>
<td>Interconnection Security Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISSO</td>
<td>Information Systems Security Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITCP</td>
<td>IT Contingency Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JBOD</td>
<td>Just a Bunch Of Disks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KDC</td>
<td>Key Distribution Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KEK</td>
<td>Key Encryption Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEAP</td>
<td>Lightweight Extensible Authentication Protocol</td>
</tr>
<tr>
<td>MaaS</td>
<td>Monitoring as a Service</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control or Media Access Control</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>MBR</td>
<td>Master Boot Record</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Frame</td>
</tr>
<tr>
<td>MITM</td>
<td>Man-In-The-Middle</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum Of Understanding</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi-Protocol Layer Switch</td>
</tr>
<tr>
<td>MSCHAP</td>
<td>Microsoft Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Recover</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time To Failure</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>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 and Technology</td>
</tr>
<tr>
<td>NOS</td>
<td>Network Operating System</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>NTLM</td>
<td>New Technology LANMAN</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>OLA</td>
<td>Open License Agreement</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OVAL</td>
<td>Open Vulnerability Assessment Language</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer to Peer</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>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>PED</td>
<td>Personal Electronic Device</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</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>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>Recovery Agent</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</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>SAS</td>
<td>Remote Access Server</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-Based Access Control</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-Based Access Control</td>
</tr>
<tr>
<td>RC4</td>
<td>RSA Variable Key Size Encryption Algorithm</td>
</tr>
<tr>
<td>RIPEMD</td>
<td>RACE Integrity Primitives Evaluation Message Digest</td>
</tr>
<tr>
<td>ROI</td>
<td>Return On Investment</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir and Adleman</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</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>SAML</td>
<td>Security Assertions Markup Language</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</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>SCSI</td>
<td>Small Computer System Interface</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>SEH</td>
<td>Structured Exception Handler</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secured File Transfer Protocol</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>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SLE</td>
<td>Single Loss Expectancy</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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SONET</td>
<td>Synchronous Optical Network Technologies</td>
</tr>
<tr>
<td>SPIM</td>
<td>Spam over Internet Messaging</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On</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>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>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>URI</td>
<td>Uniform Resource Identifier</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>UTM</td>
<td>Unified Threat Management</td>
</tr>
<tr>
<td>UTP</td>
<td>Unshielded Twisted Pair</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtualization Desktop Infrastructure</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VLSM</td>
<td>Variable Length Subnet Masking</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VTC</td>
<td>Video Teleconferencing</td>
</tr>
<tr>
<td>WAF</td>
<td>Web-Application Firewall</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Access Point</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WIDS</td>
<td>Wireless Intrusion Detection System</td>
</tr>
<tr>
<td>WIPS</td>
<td>Wireless Intrusion Prevention System</td>
</tr>
<tr>
<td>WPA</td>
<td>Wireless Protected Access</td>
</tr>
<tr>
<td>WPA2</td>
<td>WiFi Protected Access 2</td>
</tr>
<tr>
<td>WPS</td>
<td>WiFi Protected Setup</td>
</tr>
<tr>
<td>WTLS</td>
<td>Wireles TLS</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>XSRF</td>
<td>Cross-Site Request Forgery</td>
</tr>
<tr>
<td>XSS</td>
<td>Cross-Site Scripting</td>
</tr>
<tr>
<td>XTACACS</td>
<td>Extended Terminal Access Controller Access Control System</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 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
- All-in-one appliance
- Enterprise security managers/SIEM suite
- Load balancer

**SOFTWARE**
- BackTrack
- Proxy server
- Kali/BackTrack
- Virtualization software
- Virtualized appliances
- Wireshark
- TCPdump
- NMAP
- OpenVAS
- Metasploit
- Back Orifice
- Cain & Abel
- John the Ripper
- pfSense
- Security Onion
- Roo
- Any UTM

**SPARE PARTS/HARDWARE**
- Keyboards, mice
- Network cables
- Monitors

**TOOLS**
- WiFi analyzers

**OTHER**
- SourceForge

© 2016 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 01754-Feb2016