



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 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	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:

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Network Security	20%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	20%
4.0 Application, Data and Host Security	15%
5.0 Access Control and Identity Management	15%
6.0 Cryptography	12%
Total	100%



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.

- | | | |
|---|--|--|
| <ul style="list-style-type: none"> • Protocols - IPSec - SNMP - SSH - DNS - TLS - SSL - TCP/IP - FTPS - HTTPS - SCP - ICMP | <ul style="list-style-type: none"> - IPv4 - IPv6 - iSCSI - Fibre Channel - FCoE - FTP - SFTP - TFTP - TELNET - HTTP - NetBIOS | <ul style="list-style-type: none"> • Ports - 21 - 22 - 25 - 53 - 80 - 110 - 139 - 143 - 443 - 3389 • OSI relevance |
|---|--|--|

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

- | | | |
|---|---|--|
| <ul style="list-style-type: none"> • WPA • WPA2 • WEP • EAP • PEAP • LEAP | <ul style="list-style-type: none"> • MAC filter • Disable SSID broadcast • TKIP • CCMP • Antenna placement • Power level controls | <ul style="list-style-type: none"> • Captive portals • Antenna types • Site surveys • VPN (over open wireless) |
|---|---|--|



2.0 Compliance and Operational Security

2.1 Explain the importance of risk related concepts.

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

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

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

2.3 Given a scenario, implement appropriate risk mitigation strategies.

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



2.4 Given a scenario, implement basic forensic procedures.

- Order of volatility
- Capture system image
- Network traffic and logs
- Capture video
- Record time offset
- Take hashes
- Screenshots
- Witnesses
- Track man hours and expense
- Chain of custody
- Big Data analysis

2.5 Summarize common incident response procedures.

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

2.6 Explain the importance of security related awareness and training.

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

2.7 Compare and contrast physical security and environmental controls.

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



2.8 Summarize risk management best practices.

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

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

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



3.0 Threats and Vulnerabilities

3.1 Explain types of malware.

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

3.2 Summarize various types of attacks.

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

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

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

3.4 Explain types of wireless attacks.

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



3.5 Explain types of application attacks.

- Cross-site scripting
- SQL injection
- LDAP injection
- XML injection
- Directory traversal/command injection
- Buffer overflow
- Integer overflow
- Zero-day
- Cookies and attachments
- 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
- **Hardening**
 - Disabling unnecessary services
 - Protecting management interfaces and applications
 - Password protection
 - Disabling unnecessary accounts
- **Network security**
 - MAC limiting and filtering
 - 802.1X
 - Disabling unused interfaces and unused application service ports
 - Rogue machine detection
- **Security posture**
 - Initial baseline configuration
 - Continuous security monitoring
 - Remediation
- **Reporting**
 - Alarms
 - Alerts
 - Trends
- **Detection controls vs. prevention controls**
 - IDS vs. IPS
 - Camera vs. guard

3.7 Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.

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

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



4.4 Implement the appropriate controls to ensure data security.

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

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

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



5.0 Access Control and Identity Management

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

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

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

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

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

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



6.0 Cryptography

6.1 Given a scenario, utilize general cryptography concepts.

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

6.2 Given a scenario, use appropriate cryptographic methods.

- WEP vs. WPA/WPA2 and 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

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.

ACRONYM	SPELLED OUT	ACRONYM	SPELLED OUT
3DES	Triple Digital Encryption Standard	CIRT	Computer Incident Response Team
AAA	Authentication, Authorization and Accounting	CMS	Content Management System
ACL	Access Control List	COOP	Continuity Of Operation Planning
AES	Advanced Encryption Standard	CP	Contingency Planning
AES256	Advanced Encryption Standards 256-bit	CRC	Cyclical Redundancy Check
AH	Authentication Header	CRL	Certificate Revocation List
ALE	Annualized Loss Expectancy	CRM	Customer Relationship Management
AP	Access Point	CSO	Chief Security Officer
API	Application Programming Interface	CSP	Cloud Service Provider
APT	Advanced Persistent Threat	CSR	Certificate Signing Request
ARO	Annualized Rate of Occurrence	CSRF	Cross-Site Request Forgery
ARP	Address Resolution Protocol	CSU	Channel Service Unit
ASLR	Address Space Layout Randomization	CTO	Chief Technology Officer
ASP	Application Service Provider	DAC	Discretionary Access Control
AUP	Acceptable Use Policy	DBA	Database Administrator
AV	Antivirus	DDoS	Distributed Denial of Service
BAC	Business Availability Center	DEP	Data Execution Prevention
BCP	Business Continuity Planning	DES	Digital Encryption Standard
BIA	Business Impact Analysis	DHCP	Dynamic Host Configuration Protocol
BIOS	Basic Input/Output System	DHE	Data-Handling Electronics
BPA	Business Partners Agreement	DHE	Diffie-Hellman Ephemeral
BPDU	Bridge Protocol Data Unit	DLL	Dynamic Link Library
BYOD	Bring Your Own Device	DLP	Data Loss Prevention
CA	Certificate Authority	DMZ	Demilitarized Zone
CAC	Common Access Card	DNAT	Destination Network Address Transaction
CAN	Controller Area Network	DNS	Domain Name Service (Server)
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart	DoS	Denial of Service
CAR	Corrective Action Report	DRP	Disaster Recovery Plan
CCMP	Counter-mode/CBC-MAC Protocol	DSA	Digital Signature Algorithm
CCTV	Closed-Circuit Television	DSL	Digital Subscriber Line
CERT	Computer Emergency Response Team	DSU	Data Service Unit
CFB	Cipher Feedback	EAP	Extensible Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol	ECC	Elliptic Curve Cryptography
CIO	Chief Information Officer	ECDHE	Elliptic Curve Diffie-Hellman Exchange
		ECDSA	Elliptic Curve Digital Signature Algorithm

ACRONYM	SPELLED OUT	ACRONYM	SPELLED OUT
EFS	Encrypted File System	IRP	Incident Response Procedure
EMI	Electromagnetic Interference	ISA	Interconnection Security Agreement
ERP	Enterprise Resource Planning	ISP	Internet Service Provider
ESN	Electronic Serial Number	ISSO	Information Systems Security Officer
ESP	Encapsulated Security Payload	ITCP	IT Contingency Plan
FACL	File system Access Control List	IV	Initialization Vector
FDE	Full Disk Encryption	JBOD	Just a Bunch Of Disks
FQDN	Fully Qualified Domain Name	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 or Media Access Control
GPU	Graphic Processing Unit	MAC	Message Authentication Code
GRE	Generic Routing Encapsulation	MAN	Metropolitan Area Network
HA	High Availability	MBR	Master Boot Record
HDD	Hard Disk Drive	MD5	Message Digest 5
HIDS	Host-based Intrusion Detection System	MDF	Main Distribution Frame
HIPS	Host-based Intrusion Prevention System	MITM	Man-In-The-Middle
HMAC	Hashed Message Authentication Code	MOU	Memorandum Of Understanding
HOTP	HMAC-based One Time Password	MPLS	Multi-Protocol Layer Switch
HSM	Hardware Security Module	MSCHAP	Microsoft Challenge Handshake Authentication Protocol
HSRP	Hot Standby Router Protocol	MTBF	Mean Time Between Failures
HTML	Hypertext Markup Language	MTTR	Mean Time To Recover
HTTP	Hypertext Transfer Protocol	MTTF	Mean Time To Failure
HTTPS	Hypertext Transfer Protocol over SSL	MTU	Maximum Transmission Unit
HVAC	Heating, Ventilation and Air Conditioning	NAC	Network Access Control
IaaS	Infrastructure as a Service	NAT	Network Address Translation
ICMP	Internet Control Message Protocol	NDA	Non-Disclosure Agreement
ICS	Industrial Control Systems	NFC	Near Field Communication
ID	Identification	NIDS	Network-based Intrusion Detection System
IDEA	International Data Encryption Algorithm	NIPS	Network-based Intrusion Prevention System
IDF	Intermediate Distribution Frame	NIST	National Institute of Standards and Technology
IdP	Identity Provider	NOS	Network Operating System
IDS	Intrusion Detection System	NTFS	New Technology File System
IKE	Internet Key Exchange	NTLM	New Technology LANMAN
IM	Instant Messaging	NTP	Network Time Protocol
IMAP4	Internet Message Access Protocol v4	OAuth	Open Authorization
IoT	Internet of Things	OCSF	Online Certificate Status Protocol
IP	Internet Protocol	OLA	Open License Agreement
IPSec	Internet Protocol Security	OS	Operating System
IR	Incident Response	OVAL	Open Vulnerability Assessment Language
IRC	Internet Relay Chat		

ACRONYM	SPELLED OUT	ACRONYM	SPELLED OUT
P2P	Peer to Peer	SEH	Structured Exception Handler
PAC	Proxy Auto Configuration	SHA	Secure Hashing Algorithm
PAM	Pluggable Authentication Modules	SFTP	Secured File Transfer Protocol
PAP	Password Authentication Protocol	SHTTP	Secure Hypertext Transfer Protocol
PAT	Port Address Translation	SIEM	Security Information and Event Management
PBKDF2	Password-Based Key Derivation Function 2	SIM	Subscriber Identity Module
PBX	Private Branch Exchange	SLA	Service Level Agreement
PCAP	Packet Capture	SLE	Single Loss Expectancy
PEAP	Protected Extensible Authentication Protocol	SMS	Short Message Service
PED	Personal Electronic Device	SMTP	Simple Mail Transfer Protocol
PFS	Perfect Forward Secrecy	SMTSPS	Simple Mail Transfer Protocol Secure
PGP	Pretty Good Privacy	SNMP	Simple Network Management Protocol
PII	Personally Identifiable Information	SOAP	Simple Object Access Protocol
PIV	Personal Identity Verification	SONET	Synchronous Optical Network Technologies
PKI	Public Key Infrastructure	SPIM	Spam over Internet Messaging
POTS	Plain Old Telephone Service	SQL	Structured Query Language
PPP	Point-to-Point Protocol	SSD	Solid State Drive
PPTP	Point-to-Point Tunneling Protocol	SSH	Secure Shell
PSK	Pre-Shared Key	SSL	Secure Sockets Layer
PTZ	Pan-Tilt-Zoom	SSO	Single Sign-On
RA	Recovery Agent	STP	Shielded Twisted Pair or Spanning Tree Protocol
RA	Registration Authority		
RAD	Rapid Application Development	TACACS+	Terminal Access Controller Access Control System Plus
RADIUS	Remote Authentication Dial-In User Server		
RAID	Redundant Array of Inexpensive Disks	TCP/IP	Transmission Control Protocol/Internet Protocol
RAS	Remote Access Server	TFTP	Trivial File Transfer Protocol
RBAC	Role-Based Access Control	TGT	Ticket Granting Ticket
RBAC	Rule-Based Access Control	TKIP	Temporal Key Integrity Protocol
RC4	RSA Variable Key Size Encryption Algorithm	TLS	Transport Layer Security
RDP	Remote Desktop Protocol	TOTP	Time-based One-Time Password
RIPEMD	RACE Integrity Primitives Evaluation Message Digest	TPM	Trusted Platform Module
ROI	Return On Investment	TSIG	Transaction Signature
RPO	Recovery Point Objective	UAT	User Acceptance Testing
RSA	Rivest, Shamir and Adleman	UEFI	Unified Extensible Firmware Interface
RTBH	Remote Triggered Black Hole	UDP	User Datagram Protocol
RTO	Recovery Time Objective	UPS	Uninterruptable Power Supply
RTP	Real-time Transport Protocol	URI	Uniform Resource Identifier
S/MIME	Secure/Multipurpose Internet Mail Extensions	URL	Universal Resource Locator
SAML	Security Assertions Markup Language	USB	Universal Serial Bus
SaaS	Software as a Service	UTM	Unified Threat Management
SAN	Storage Area Network	UTP	Unshielded Twisted Pair
SCADA	System Control and Data Acquisition	VDI	Virtualization Desktop Infrastructure
SCAP	Security Content Automation Protocol	VLAN	Virtual Local Area Network
SCEP	Simple Certificate Enrollment Protocol	VLSM	Variable Length Subnet Masking
SCSI	Small Computer System Interface	VM	Virtual Machine
SDLC	Software Development Life Cycle	VoIP	Voice over IP
SDLM	Software Development Life Cycle Methodology	VPN	Virtual Private Network

ACRONYM	SPELLED OUT
VTC	Video Teleconferencing
WAF	Web-Application Firewall
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WPA	WiFi Protected Access
WPA2	WiFi Protected Access 2
WPS	WiFi Protected Setup
WTLS	Wireless TLS
XML	Extensible Markup Language
XSRF	Cross-Site Request Forgery
XSS	Cross-Site Scripting

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

SPARE PARTS/HARDWARE

- Keyboards, mice
- Network cables
- Monitors

TOOLS

- WiFi analyzers

SOFTWARE

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

OTHER

- SourceForge