CompTIA Security+ Certification Exam Objectives

EXAM NUMBER: SY0-601
About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Security+ (SY0-601) certification exam. The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to:

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions
- Monitor and secure hybrid environments, including cloud, mobile, and IoT
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance
- Identify, analyze, and respond to security events and incidents

This is equivalent to two years of hands-on experience working in a security/systems administrator job role. These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

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 testing exam objectives. Please know that all related exam preparation materials will still be valid.
TEST DETAILS

Required exam: SY0-601
Number of questions: Maximum of 90
Types of questions: Multiple choice and performance-based
Length of test: 90 minutes
Recommended experience:
- At least 2 years of work experience in IT systems administration with a focus on security
- Hands-on technical information security experience
- Broad knowledge of security concepts
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 Attacks, Threats, and Vulnerabilities</td>
<td>24%</td>
</tr>
<tr>
<td>2.0 Architecture and Design</td>
<td>21%</td>
</tr>
<tr>
<td>3.0 Implementation</td>
<td>25%</td>
</tr>
<tr>
<td>4.0 Operations and Incident Response</td>
<td>16%</td>
</tr>
<tr>
<td>5.0 Governance, Risk, and Compliance</td>
<td>14%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
1.0 Threats, Attacks, and Vulnerabilities

1.1 Compare and contrast different types of social engineering techniques.

- Phishing
- Smishing
- Vishing
- Spam
- Spam over Internet messaging (SPIM)
- Spear phishing
- Dumpster diving
- Shoulder surfing
- Phishing
- Tailgating
- Eliciting information
- Whaling
- Prepending
- Identity fraud
- Invoice scams
- Credential harvesting
- Reconnaissance
- Hoax
- Impersonation
- Watering hole attack
- Typo squatting
- Pretexting
- Influence campaigns
  - Hybrid warfare
  - Social media
  - Principles (reasons for effectiveness)
    - Authority
    - Intimidation
    - Consensus
    - Scarcity
    - Familiarity
    - Trust
    - Urgency

1.2 Given a scenario, analyze potential indicators to determine the type of attack.

- Malware
  - Ransomware
  - Trojans
  - Worms
  - Potentially unwanted programs (PUPs)
  - Fileless virus
  - Command and control
  - Bots
  - Cryptomalware
  - Logic bombs
  - Spyware
  - Keyloggers
  - Remote access Trojan (RAT)
  - Rootkit
  - Backdoor

- Password attacks
  - Spraying
  - Dictionary
  - Brute force
  - Offline
  - Online
  - Rainbow tables
  - Plaintext/unencrypted

- Physical attacks
  - Malicious universal serial bus (USB) cable
  - Malicious flash drive
  - Card cloning
  - Skimming

- Adversarial artificial intelligence (AI)
  - Tainted training data for machine learning (ML)
  - Security of machine learning algorithms

- Supply-chain attacks

- Cryptographic attacks
  - Birthday
  - Collision
  - Downgrade
## 1.3 Given a scenario, analyze potential indicators associated with application attacks.

- Privilege escalation
- Cross-site scripting
- Injections
  - Structured query language (SQL)
  - Dynamic link library (DLL)
  - Lightweight directory access protocol (LDAP)
  - Extensible markup language (XML)
- Pointer/object dereference
- Directory traversal
- Buffer overflows
- Race conditions
  - Time of check/time of use
- Error handling
- Improper input handling
- Replay attack
  - Session replays
- Integer overflow
- Request forgeries
  - Server-side
  - Client-side
  - Cross-site
- Application programming interface (API) attacks
- Resource exhaustion
- Memory leak
- Secure sockets layer (SSL) stripping
- Driver manipulation
  - Shimming
  - Refactoring
- Pass the hash

## 1.4 Given a scenario, analyze potential indicators associated with network attacks.

- Wireless
  - Evil twin
  - Rogue access point
  - Bluesnarfing
  - Bluejacking
  - Disassociation
  - Jamming
  - Radio frequency identifier (RFID)
  - Near-field communication (NFC)
  - Initialization vector (IV)
- Man-in-the-middle
- Man-in-the-browser
- Layer 2 attacks
  - Address resolution protocol (ARP) poisoning
  - Media access control (MAC) flooding
  - MAC cloning
- Domain name system (DNS)
  - Domain hijacking
  - DNS poisoning
  - Universal resource locator (URL) redirection
- Domain reputation
- Distributed denial-of-service (DDoS)
  - Network
  - Application
  - Operational technology (OT)
- Malicious code or script execution
  - PowerShell
  - Python
  - Bash
  - Macros
  - Virtual Basic for Applications (VBA)
1.5 Explain different threat actors, vectors, and intelligence sources.

- **Actors and threats**
  - Advanced persistent threat (APT)
  - Insider threats
  - State actors
  - Hacktivists
  - Script kiddies
  - Criminal syndicates
  - Hackers
    - White hat
    - Black hat
    - Gray hat
  - Shadow IT
  - Competitors

- **Vectors**
  - Direct access
  - Wireless
  - Email
  - Supply chain
  - Social media
  - Removable media
  - Cloud

- **Threat intelligence sources**
  - Open source intelligence (OSINT)
  - Closed/proprietary
  - Vulnerability databases
  - Public/private information-sharing centers
  - Dark web
  - Indicators of compromise

- **Attributes of actors**
  - Internal/external
  - Level of sophistication/capability
  - Resources/funding
  - Intent/motivation

1.6 Explain the security concerns associated with various types of vulnerabilities.

- **Cloud-based vs. on-premises vulnerabilities**
- **Zero-day**
- **Weak configurations**
  - Open permissions
  - Unsecure root accounts
  - Errors
  - Weak encryption
  - Unsecure protocols
  - Default settings
  - Open ports and services

- **Third-party risks**
  - Vendor management
    - System integration
    - Lack of vendor support
  - Supply chain
  - Outsourced code development
  - Data storage

- **Improper or weak patch management**
  - Firmware
  - Operating system (OS)
  - Applications

- **Legacy platforms**
- **Impacts**
  - Data loss
  - Data breaches
  - Data exfiltration
  - Identity theft
  - Financial
  - Reputation
  - Availability loss
1.7 Summarize the techniques used in security assessments.

- Threat hunting
  - Intelligence fusion
  - Threat feeds
  - Advisories and bulletins
  - Maneuver
- Vulnerability scans
  - False positives
  - False negatives
  - Log reviews
  - Credentialled vs. non-credentialled
  - Intrusive vs. non-intrusive
  - Application
  - Web application
  - Network
  - Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)
  - Configuration review
- Syslog/Security information and event management (SIEM)
  - Review reports
  - Packet capture
  - Data inputs
  - User behavior analysis
  - Sentiment analysis
  - Security monitoring
  - Log aggregation
  - Log collectors
- Security orchestration, automation, and response (SOAR)

1.8 Explain the techniques used in penetration testing.

- Penetration testing
  - White-box
  - Black-box
  - Gray-box
  - Rules of engagement
  - Lateral movement
  - Privilege escalation
  - Persistence
  - Cleanup
  - Bug bounty
  - Pivoting
- Passive and active reconnaissance
  - Drones/unmanned aerial vehicle (UAV)
  - War flying
  - War driving
  - Footprinting
  - OSINT
- Exercise types
  - Red-team
  - Blue-team
  - White-team
  - Purple-team
2.0 Architecture and Design

2.1 Explain the importance of security concepts in an enterprise environment.

- Configuration management
  - Diagrams
  - Baseline configuration
  - Standard naming conventions
  - Internet protocol (IP) schema
- Data sovereignty
- Data protection
  - Data loss prevention (DLP)
  - Masking
  - Encryption
  - At rest
  - In transit/motion
  - In processing
  - Tokenization
  - Rights management
- Hardware security module (HSM)
- Geographical considerations
- Cloud access security broker (CASB)
- Response and recovery controls
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection
- Hashing
- API considerations
- Site resiliency
  - Hot site
  - Cold site
  - Warm site
- Deception and disruption
  - Honeypots
  - Honeyfiles
  - Honeynets
  - Fake telemetry
  - DNS sinkhole

2.2 Summarize virtualization and cloud computing concepts.

- Cloud models
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)
  - Anything as a service (XaaS)
  - Public
  - Community
  - Private
  - Hybrid
- Managed service provider (MSP)/managed security service provider (MSSP)
- On-premises vs. off-premises
- Fog computing
- Edge computing
- Thin client
- Containers
- Microservices/API
- Infrastructure as code
  - Software-defined networking (SDN)
  - Software-defined visibility (SDV)
- Serverless architecture
- Services integration
- Resource policies
- Transit gateway
- Virtualization
  - Virtual machine (VM)
  - sprawl avoidance
  - VM escape protection
2.3 Summarize secure application development, deployment, and automation concepts.

- Environment
  - Development
  - Test
  - Staging
  - Production
  - Quality assurance (QA)
- Provisioning and deprovisioning
- Integrity measurement
- Secure coding techniques
  - Normalization
  - Stored procedures
  - Obfuscation/camouflage
- Code reuse/dead code
- Server-side vs. client-side execution and validation
- Memory management
- Use of third-party libraries and software development kits (SDKs)
- Data exposure
- Open Web Application Security Project (OWASP)
- Software diversity
  - Compiler
  - Binary
- Automation/scripting
  - Automated courses of action
  - Continuous monitoring
  - Continuous validation
  - Continuous integration
  - Continuous delivery
  - Continuous deployment
- Elasticity
- Scalability
- Version control

2.4 Summarize authentication and authorization design concepts.

- Authentication methods
  - Directory services
  - Federation
  - Attestation
  - Technologies
    - Time-based one-time password (TOTP)
    - HMAC-based one-time password (HOTP)
    - Short message service (SMS)
    - Token key
    - Static codes
    - Authentication applications
    - Push notifications
    - Phone call
    - Smart card authentication
- Biometrics
  - Fingerprint
  - Retina
  - Iris
  - Facial
  - Voice
  - Vein
  - Gait analysis
  - Efficacy rates
  - False acceptance
  - False rejection
  - Crossover error rate
- Multifactor authentication (MFA) factors and attributes
  - Factors
    - Something you know
    - Something you have
    - Something you are
  - Attributes
    - Somewhere you are
    - Something you can do
    - Something you exhibit
    - Someone you know
- Authentication, authorization, and accounting (AAA)
- Cloud vs. on-premises requirements
Given a scenario, implement cybersecurity resilience.

- **Redundancy**
  - Geographic dispersal
  - Disk
    - Redundant array of inexpensive disks (RAID) levels
  - Multipath
  - Network
    - Load balancers
    - Network interface card (NIC) teaming
  - Power
    - Uninterruptible power supply (UPS)
  - Generator
  - Dual supply
  - Managed power distribution units (PDUs)
- **Replication**
  - Storage area network
  - VM
- **On-premises vs. cloud**
- **Backup types**
  - Full
  - Incremental
  - Snapshot
  - Differential
  - Tape
  - Disk
  - Copy
  - Network-attached storage (NAS)
  - Storage area network
  - Cloud
  - Image
  - Online vs. offline
- **Offsite storage**
  - Distance considerations
- **Non-persistence**
  - Revert to known state
  - Last known-good configuration
  - Live boot media
- **High availability**
  - Scalability
- **Restoration order**
- **Diversity**
  - Technologies
  - Vendors
  - Crypto
  - Controls

Explain the security implications of embedded and specialized systems.

- **Embedded systems**
  - Raspberry Pi
  - Field-programmable gate array (FPGA)
  - Arduino
- **Supervisory control and data acquisition (SCADA)/industrial control system (ICS)**
  - Facilities
  - Industrial
  - Manufacturing
  - Energy
  - Logistics
- **Internet of Things (IoT)**
  - Sensors
  - Smart devices
  - Wearables
  - Facility automation
  - Weak defaults
- **Specialized**
  - Medical systems
  - Vehicles
  - Aircraft
  - Smart meters
- **Voice over IP (VoIP)**
- **Heating, ventilation, air conditioning (HVAC)**
- **Drones/AVs**
- **Multifunction printer (MFP)**
- **Real-time operating system (RTOS)**
- **Surveillance systems**
- **System on chip (SoC)**
- **Communication considerations**
  - 5G
  - Narrow-band
  - Baseband radio
- **Subscriber identity module (SIM) cards**
  - Zigbee
- **Constraints**
  - Power
  - Compute
  - Network
  - Crypto
  - Inability to patch
  - Authentication
  - Range
  - Cost
  - Implied trust
## 2.7 Explain the importance of physical security controls.

- Bollards/barricades
- Mantraps
- Badges
- Alarms
- Signage
- Cameras
  - Motion recognition
  - Object detection
- Closed-circuit television (CCTV)
- Industrial camouflage
- Personnel
  - Guards
  - Robot sentries
  - Reception
  - Two-person integrity/control
- Locks
  - Biometrics
- Electronic
- Physical
- Cable locks
- USB data blocker
- Lighting
- Fencing
- Fire suppression
- Sensors
  - Motion detection
  - Noise detection
  - Proximity reader
  - Moisture detection
  - Cards
  - Temperature
- Closed-circuit television (CCTV)
- Industrial camouflage
- Personnel
  - Guards
  - Robot sentries
  - Reception
  - Two-person integrity/control
- Locks
  - Biometrics
- Electronic
  - Physical
  - Cable locks
- USB data blocker
- Lighting
- Fencing
- Fire suppression
- Sensors
  - Motion detection
  - Noise detection
  - Proximity reader
  - Moisture detection
  - Cards
  - Temperature
- Air gap
- Demilitarized zone (DMZ)
- Protected cable distribution
- Secure areas
  - Air gap
  - Vault
  - Safe
  - Hot aisle
  - Cold aisle
- Secure data destruction
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Third-party solutions

## 2.8 Summarize the basics of cryptographic concepts.

- Digital signatures
- Key length
- Key stretching
- Salting
- Hashing
- Key exchange
- Elliptic-curve cryptography
- Perfect forward secrecy
- Quantum
  - Communications
  - Computing
- Post-quantum
- Ephemeral
- Modes of operation
  - Authenticated
  - Unauthenticated
  - Counter
- Blockchain
  - Public ledgers
- Cipher suites
  - Stream
  - Block
- Symmetric vs. asymmetric
- Lightweight cryptography
- Steganography
  - Audio
  - Video
  - Image
- Homomorphic encryption
- Common use cases
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality
- Anew
- Supporting integrity
- Supporting obfuscation
- Supporting authentication
- Supporting non-repudiation
- Resource vs. security constraints
- Limitations
  - Speed
  - Size
  - Weak keys
  - Time
  - Longevity
  - Predictability
  - Reuse
  - Entropy
  - Computational overheads
  - Resource vs. security constraints
### 3.0 Implementation

#### 3.1 Given a scenario, implement secure protocols.

**Protocols**
- Domain Name System Security Extension (DNSSEC)
- SSH
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Secure Real-time Protocol (SRTP)
- Lightweight Directory Access Protocol Over SSL (LDAPS)
- File Transfer Protocol, Secure (FTPS)
- SSH File Transfer Protocol (SFTP)
- Simple Network Management Protocol, version 3 (SNMPv3)
- Hypertext transfer protocol over SSL/TLS (HTTPS)
- IPsec
  - Authentication header (AH)/Encapsulating Security Payloads (ESP)
- Tunnel/transport
- Secure Post Office Protocol (POP)/Internet Message Access Protocol (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

#### 3.2 Given a scenario, implement host or application security solutions.

**Endpoint protection**
- Antivirus
- Anti-malware
- Endpoint detection and response (EDR)
- DLP
- Next-generation firewall (NGFW)
- Host-based intrusion prevention system (HIPS)
- Host-based intrusion detection system (HIDS)
- Host-based firewall

**Boot integrity**
- Boot security/Unified Extensible Firmware Interface (UEFI)
- Measured boot

**Database**
- Tokenization
- Salting
- Hashing

**Application security**
- Input validations
- Secure cookies
- Hypertext Transfer Protocol (HTTP) headers
- Code signing
- Whitelisting
- Blacklisting
- Secure coding practices
- Static code analysis
  - Manual code review

**Hardening**
- Open ports and services
- Registry
- Disk encryption
- OS
- Patch management
  - Third-party updates
  - Auto-update
- Self-encrypting drive (SED)/full-disk encryption (FDE)
- Opal
- Hardware root of trust
- Trusted Platform Module (TPM)
- Sandboxing
Given a scenario, implement secure network designs.

- Load balancing
  - Active/active
  - Active/passive
  - Scheduling
  - Virtual IP
  - Persistence

- Network segmentation
  - Virtual local area network (VLAN)
  - DMZ
  - East-west traffic
  - Extranet
  - Intranet
  - Zero Trust

- Virtual private network (VPN)
  - Always-on
  - Split tunnel vs. full tunnel
  - Remote access vs. site-to-site
  - IPSec
  - SSL/TLS
  - HTML5
  - Layer 2 tunneling protocol (L2TP)

- DNS
  - Network access control (NAC)
    - Agent and agentless

- Out-of-band management

- Port security
  - Broadcast storm prevention
  - Bridge Protocol Data Unit (BPDU) guard
  - Loop prevention
  - Dynamic Host Configuration Protocol (DHCP) snooping
  - Media access control (MAC) filtering

- Network appliances
  - Jump servers
  - Proxy servers
    - Forward
    - Reverse
  - Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS)
    - Signature-based
    - Heuristic/behavior
    - Anomaly
    - Inline vs. passive
  - HSM
  - Sensors

- Collector
  - Aggregators
  - Firewalls
    - Web application firewall (WAF)
  - NGFW
  - Stateful
  - Stateless
  - Unified threat management (UTM)
  - Network address translation (NAT) gateway
  - Content/URL filter
  - Open-source vs. proprietary
  - Hardware vs. software
  - Appliance vs. host-based vs. virtual

- Access control list (ACL)
- Route security
- Quality of service (QoS)
- Implications of IPv6
- Port spanning/port mirroring
  - Port taps
  - Monitoring services
  - File integrity monitors

Given a scenario, install and configure wireless security settings.

- Cryptographic protocols
  - WiFi protected access II (WPA2)
  - WiFi protected access III (WPA3)
  - Counter-mode/CBC-MAC protocol (CCMP)
  - Simultaneous Authentication of Equals (SAE)

- Authentication protocols
  - Extensible Authentication Protocol (EAP)
  - Protected Extensible Application Protocol (PEAP)
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1X
  - Remote Authentication Dial-in User Service (RADIUS) Federation

- Methods
  - Pre-shared key (PSK) vs. Enterprise vs. Open
  - WiFi Protected Setup (WPS)
  - Captive portals

- Installation considerations
  - Site surveys
  - Heat maps
  - WiFi analyzers
  - Channel overlays
  - Wireless access point (WAP) placement
  - Controller and access point security
3.0 Implementation

Given a scenario, implement secure mobile solutions.

- **Connection methods and receivers**
  - Cellular
  - WiFi
  - Bluetooth
  - NFC
  - Infrared
  - USB
  - Point-to-point
  - Point-to-multipoint
  - Global Positioning System (GPS)
  - RFID
- **Mobile devices**
  - MicroSD HSM
  - MDM/Unified Endpoint Management (UEM)
  - Mobile application management (MAM)
  - SEAndroid
- **Mobile device management (MDM)**
  - Application management
  - Content management
  - Remote wipe
  - Geofencing
  - Geolocation
  - Screen locks
  - Push notifications
  - Passwords and pins
- **Biometrics**
- **Context-aware authentication**
- **Containerization**
- **Storage segmentation**
- **Full device encryption**
- **SMS/Multimedia Messaging Service (MMS)/Rich communication services (RCS)**
- **External media**
- **USB On-The-Go (USB OTG)**
- **Recording microphone**
- **GPS tagging**
- **WiFi direct/ad hoc**
- **Tethering**
- **Hotspot**
- **Payment methods**
- **Deployment models**
  - Bring your own device (BYOD)
  - Corporate-owned personally enabled (COPE)
  - Choose your own device (CYOD)
  - Corporate-owned
  - Virtual desktop infrastructure (VDI)

3.6 Given a scenario, apply cybersecurity solutions to the cloud.

- **Cloud security controls**
  - High availability across zones
  - Resource policies
  - Secrets management
  - Integration and auditing
  - Storage
    - Permissions
    - Encryption
    - Replication
    - High availability
  - Network
    - Virtual networks
    - Public and private subnets
    - Segmentation
    - API inspection and integration
  - Compute
    - Security groups
    - Dynamic resource allocation
    - Instance awareness
    - Virtual private cloud (VPC) endpoint
    - Container security
- **Solutions**
  - CASB
  - Application security
  - Next-generation Secure Web Gateway (SWG)
  - Firewall considerations in a cloud environment
    - Cost
    - Need for segmentation
    - Open Systems Interconnection (OSI) layers
- **Cloud native controls vs. third-party solutions**
3.0 Implementation

3.7 Given a scenario, implement identity and account management controls.

- **Identity**
  - Identity provider (IdP)
  - Attributes
  - Certificates
  - Tokens
  - SSH keys
  - Smart cards

- **Account policies**
  - Password complexity
  - Password history
  - Time of day
  - Network location
  - Geofencing
  - Geotagging
  - Golocation

- **Account types**
  - User account
  - Shared and generic accounts/credentials
  - Guest accounts
  - Service accounts

- **Authentication management**
  - Password keys
  - Password vaults
  - TPM
  - HSM
  - Knowledge-based authentication

- **Authentication**
  - EAP
  - Challenge Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)

- **Access control schemes**
  - Attribute-based access control (ABAC)

3.8 Given a scenario, implement authentication and authorization solutions.

- **Authentication management**
  - Password keys
  - Password vaults
  - 802.1X
  - RADIUS

- **Authentication**
  - Single sign-on (SSO)
  - Security Assertions Markup Language (SAML)
  - Terminal Access Controller Access Control System Plus (TACACS+)
  - OAuth
  - OpenID
  - Kerberos

- **Access control schemes**
  - Role-based access control
  - Rule-based access control
  - MAC
  - Discretionary access control (DAC)
  - Conditional access
  - Privilege access management
  - Filesystem permissions

3.9 Given a scenario, implement public key infrastructure.

- **Public key infrastructure (PKI)**
  - Key management
  - Certificate authority (CA)
  - Intermediate CA
  - Registration authority (RA)
  - Certificate revocation list (CRL)
  - Certificate attributes
  - Online Certificate Status Protocol (OCSP)
  - Certificate signing request (CSR)
  - CN
  - Subject alternative name
  - Expiration

- **Types of certificates**
  - Wildcard
  - Subject alternative name
  - Code signing
  - Self-signed
  - Machine/computer
  - Email
  - User
  - Root
  - Domain validation
  - Extended validation

- **Certificate formats**
  - Distinguished encoding rules (DER)

- **Concepts**
  - Online vs. offline CA
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining

CompTIA Security+ Certification Exam Objectives Version 1.0 (Exam Number: SY0-601)
4.0 Operations and Incident Response

4.1 Given a scenario, use the appropriate tool to assess organizational security.

- Network reconnaissance and discovery
  - tracert/traceroute
  - nslookup/dig
  - ipconfig/ifconfig
  - nmap
  - ping/pathping
  - hping
  - netstat
  - netcat
  - IP scanners
  - arp
  - route
  - curl
  - the harvester
  - sn1per

- File manipulation
  - head
  - tail
  - cat
  - grep
  - chmod
  - logger

- Shell and script environments
  - SSH
  - PowerShell
  - Python

- OpenSSH
- Packet capture and replay
  - Tcpreplay
  - Tcpdump
  - Wireshark

- Forensics
  - dd
  - Memdump
  - WinHex
  - FTK imager
  - Autopsy

- Exploitation frameworks
- Password crackers
- Data sanitization

4.2 Summarize the importance of policies, processes, and procedures for incident response.

- Incident response plans
- Incident response process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned

- Exercises
  - Tabletop
  - Walkthroughs
  - Simulations

- Attack frameworks
  - MITRE ATT&CK
  - The Diamond Model of Intrusion Analysis
  - Cyber Kill Chain

- Stakeholder management
- Communication plan
- Disaster recovery plan
- Business continuity plan
- Continuity of operations planning (COOP)
- Incident response team
- Retention policies
4.0 Operations and Incident Response

4.3 Given an incident, utilize appropriate data sources to support an investigation.

- Vulnerability scan output
- SIEM dashboards
  - Sensor
  - Sensitivity
  - Trends
  - Alerts
  - Correlation
- Log files
  - Network
  - System
  - Application
- Security
- Web
- DNS
- Authentication
- Dump files
- VoIP and call managers
- Session Initiation Protocol (SIP) traffic
- syslog/rsyslog/syslog-ng
- journalctl
- nxlog
- Retention
- Bandwidth monitors
- Metadata
  - Email
  - Mobile
  - Web
  - File
- Netflow/sflow
  - Echo
  - IPfix
- Protocol analyzer output

4.4 Given an incident, apply mitigation techniques or controls to secure an environment.

- Reconfigure endpoint security solutions
  - Application whitelisting
  - Application blacklisting
  - Quarantine
- Configuration changes
  - Firewall rules
  - MDM
  - DLP
  - Content filter/URL filter
  - Update or revoke certificates
- Isolation
- Containment
- Segmentation
- SOAR
  - Runbooks
  - Playbooks

4.5 Explain the key aspects of digital forensics.

- Documentation/evidence
  - Legal hold
  - Video
  - Admissibility
  - Chain of custody
  - Timelines of sequence of events
    - Time stamps
    - Time offset
  - Tags
  - Reports
  - Event logs
  - Interviews
- Acquisition
  - Order of volatility
  - Disk
  - Random-access memory (RAM)
  - Swap/pagefile
  - OS
  - Device
  - Firmware
  - Snapshot
  - Cache
  - Network
  - Artifacts
- On-premises vs. cloud
  - Right-to-audit clauses
  - Regulatory/jurisdiction
  - Data breach notification laws
- Integrity
  - Hashing
  - Checksums
  - Provenance
- Preservation
  - E-discovery
  - Data recovery
  - Non-repudiation
  - Strategic intelligence/counterintelligence
5.0 Governance, Risk, and Compliance

5.1 Compare and contrast various types of controls.

- **Category**
  - Managerial
  - Operational
  - Technical

- **Control type**
  - Preventative
  - Detective
  - Corrective
  - Deterrent
  - Compensating
  - Physical

5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.

- **Regulations, standards, and legislation**
  - General Data Protection Regulation (GDPR)
  - National, territory, or state laws
  - Payment Card Industry Data Security Standard (PCI DSS)

- **Key frameworks**
  - Center for Internet Security (CIS)
  - National Institute of Standards and Technology (NIST) RMF/CSF
  - International Organization for Standardization (ISO)
    - 27001/27002/27701/31000
    - SSAS SOC 2 Type I/II
    - Cloud security alliance
    - Cloud control matrix

- **Reference architecture**
  - Platform/vendor-specific guides
    - Web server
    - OS
    - Application server
    - Network infrastructure devices

5.3 Explain the importance of policies to organizational security.

- **Personnel**
  - Acceptable use policy
  - Job rotation
  - Mandatory vacation
  - Separation of duties
  - Least privilege
  - Clean desk space
  - Background checks
  - Non-disclosure agreement (NDA)
  - Social media analysis
  - Onboarding
  - Offboarding
  - User training
    - Gamification
    - Capture the flag
    - Phishing campaigns
    - Phishing simulations

- **Computer-based training (CBT)**
  - Role-based training

- **Diversity of training techniques**
  - Third-party risk management
    - Vendors
    - Supply chain
    - Business partners
    - Service level agreement (SLA)
    - Memorandum of understanding (MOU)
    - Measurement systems analysis (MSA)
    - Business partnership agreement (BPA)
    - End of life (EOL)
    - End of service (EOS)
    - NDA

- **Data**
  - Classification
  - Governance
  - Retention

- **Credential policies**
  - Personnel
  - Third-party
  - Devices
  - Service accounts
  - Administrator/root accounts

- **Organizational policies**
  - Change management
  - Change control
  - Asset management
5.0 Governance, Risk, and Compliance

5.4 Summarize risk management processes and concepts.

- Risk types
  - External
  - Internal
  - Legacy systems
  - Multiparty
  - IP theft
  - Software compliance/licensing
- Risk management strategies
  - Acceptance
  - Avoidance
  - Transference
    - Cybersecurity insurance
  - Mitigation
- Risk analysis
  - Risk register
  - Risk matrix/heat map
  - Risk control assessment

5.5 Explain privacy and sensitive data concepts in relation to security.

- Organizational consequences of privacy breaches
  - Reputation damage
  - Identity theft
  - Fines
  - IP theft
- Notifications of breaches
  - Escalation
  - Public notifications and disclosures
- Data types
  - Classifications
    - Public
    - Private
    - Sensitive
    - Confidential
    - Critical
    - Proprietary
  - Personally identifiable information (PII)
  - Health information
  - Financial information
  - Government data
  - Customer data
- Privacy enhancing technologies
  - Data minimization
  - Data masking
  - Tokenization
  - Anonymization
  - Pseudo-anonymization
- Roles and responsibilities
  - Data owners
  - Data controller
  - Data processor
  - Data custodian/steward
  - Data protection officer (DPO)

- Disasters
  - Environmental
  - Person-made
  - Internal vs. external
- Business impact analysis
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)
  - Functional recovery plans
  - Single point of failure
  - Disaster recovery plan (DRP)
  - Mission essential functions
  - Identification of critical systems
  - Site risk assessment

- Information life cycle
- Impact assessment
- Terms of agreement
- Privacy notice
Security+ (SY0-601) Acronym List

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>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>Triple Digital Encryption Algorithm</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
</tr>
<tr>
<td>ABAC</td>
<td>Attribute-based Access Control</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AES256</td>
<td>Advanced Encryption Standards 256bit</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AIS</td>
<td>Automated Indicator Sharing</td>
</tr>
<tr>
<td>ALE</td>
<td>Annualized Loss Expectancy</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>ARO</td>
<td>Annualized Rate of Occurrence</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>ASLR</td>
<td>Address Space Layout Randomization</td>
</tr>
<tr>
<td>ASP</td>
<td>Active Server Pages</td>
</tr>
<tr>
<td>ATT&amp;CK</td>
<td>Adversarial Tactics, Techniques, and Common Knowledge</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td>AV</td>
<td>Antivirus</td>
</tr>
<tr>
<td>BASH</td>
<td>Bourne Again Shell</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Planning</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
</tr>
<tr>
<td>BPA</td>
<td>Business Partnership Agreement</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
</tr>
<tr>
<td>BSSID</td>
<td>Basic Service Set Identifier</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CAC</td>
<td>Common Access Card</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>Completely Automated Public Turing Test to Tell Computers and Humans Apart</td>
</tr>
<tr>
<td>CAR</td>
<td>Corrective Action Report</td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher Block Chaining</td>
</tr>
<tr>
<td>CBT</td>
<td>Computer-based Training</td>
</tr>
<tr>
<td>CCMP</td>
<td>Counter-Mode/CBC-MAC Protocol</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge-Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CIRT</td>
<td>Computer Incident Response Team</td>
</tr>
<tr>
<td>CIS</td>
<td>Center for Internet Security</td>
</tr>
<tr>
<td>CMS</td>
<td>Common Management System</td>
</tr>
<tr>
<td>CN</td>
<td>Common Name</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity of Operations Planning</td>
</tr>
<tr>
<td>COPE</td>
<td>Corporate-owned Personally Enabled</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>CSA</td>
<td>Cloud Security Alliance</td>
</tr>
<tr>
<td>CSIRT</td>
<td>Computer Security Incident Response Team</td>
</tr>
<tr>
<td>CSO</td>
<td>Chief Security Officer</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>CSR</td>
<td>Certificate Signing Request</td>
</tr>
<tr>
<td>CSRF</td>
<td>Cross-Site Request Forgery</td>
</tr>
<tr>
<td>CSU</td>
<td>Channel Service Unit</td>
</tr>
<tr>
<td>CTM</td>
<td>Counter-Mode</td>
</tr>
<tr>
<td>CTO</td>
<td>Chief Technology Officer</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures</td>
</tr>
<tr>
<td>CVSS</td>
<td>Common Vulnerability Scoring System</td>
</tr>
<tr>
<td>CYOD</td>
<td>Choose Your Own Device</td>
</tr>
<tr>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>DBA</td>
<td>Database Administrator</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial-of-Service</td>
</tr>
<tr>
<td>DEP</td>
<td>Data Execution Prevention</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>DER</td>
<td>Distinguished Encoding Rules</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DHE</td>
<td>Diffie-Hellman Ephemeral</td>
</tr>
<tr>
<td>DKIM</td>
<td>Domain Keys Identified Mail</td>
</tr>
<tr>
<td>DLL</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>DMARC</td>
<td>Domain Message Authentication Reporting and Conformance</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DNAT</td>
<td>Destination Network Address Transaction</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>Domain Name System Security Extensions</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial-of-Service</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Code Book</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic-curve Cryptography</td>
</tr>
<tr>
<td>ECDHE</td>
<td>Elliptic-curve Diffie-Hellman Ephemeral</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic-curve Digital Signature Algorithm</td>
</tr>
<tr>
<td>EDR</td>
<td>Endpoint Detection and Response</td>
</tr>
<tr>
<td>EFS</td>
<td>Encrypted File System</td>
</tr>
<tr>
<td>EIP</td>
<td>Extended Instruction Pointer</td>
</tr>
<tr>
<td>EOL</td>
<td>End of Life</td>
</tr>
<tr>
<td>EOS</td>
<td>End of Service</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
</tr>
<tr>
<td>ESN</td>
<td>Electronic Serial Number</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>ESSID</td>
<td>Extended Service Set Identifier</td>
</tr>
<tr>
<td>FACL</td>
<td>File System Access Control List</td>
</tr>
<tr>
<td>FDE</td>
<td>Full Disk Encryption</td>
</tr>
<tr>
<td>FIM</td>
<td>File Integrity Monitoring</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable Gate Array</td>
</tr>
<tr>
<td>FRR</td>
<td>False Rejection Rate</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>FTPS</td>
<td>Secured File Transfer Protocol</td>
</tr>
<tr>
<td>GCM</td>
<td>Galois/Counter Mode</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GPG</td>
<td>GNU Privacy Guard</td>
</tr>
<tr>
<td>GPO</td>
<td>Group Policy Object</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host-based Intrusion Detection System</td>
</tr>
<tr>
<td>HIPS</td>
<td>Host-based Intrusion Prevention System</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hash-based Message Authentication Code</td>
</tr>
</tbody>
</table>

ACRONYM  DEFINITION
HOTP     HMAC-based One-time Password
HSM      Hardware Security Module
HSMaasS  Hardware Security Module as a Service
HTML     Hypertext Markup Language
HTTP     Hypertext Transfer Protocol
HTTPS    Hypertext Transfer Protocol Secure
HVAC     Heating, Ventilation, Air Conditioning
IaaS      Infrastructure as a Service
IAM      Identity and Access Management
ICMP    Internet Control Message Protocol
ICS      Industrial Control Systems
IDEA     International Data Encryption Algorithm
IDF      Intermediate Distribution Frame
IdP      Identity Provider
IDS      Intrusion Detection System
IEEE     Institute of Electrical and Electronics Engineers
IKE      Internet Key Exchange
IM       Instant Messaging
IMAP4    Internet Message Access Protocol v4
IoC      Indicators of Compromise
IoT      Internet of Things
IP       Internet Protocol
IPS      Intrusion Prevention System
IPSec    Internet Protocol Security
IR       Incident Response
IRC      Internet Relay Chat
IRP      Incident Response Plan
ISA      Interconnection Security Agreement
ISFW     Internal Segmentation Firewall
ISO      International Organization for Standardization
ISP      Internet Service Provider
ISSO     Information Systems Security Officer
ITCP     IT Contingency Plan
IV       Initialization Vector
KDC      Key Distribution Center
KEK      Key Encryption Key
L2TP     Layer 2 Tunneling Protocol
LAN      Local Area Network
LDAP     Lightweight Directory Access Protocol
LEAP     Lightweight Extensible Authentication Protocol
MaaS     Monitoring as a Service
MAC      Media Access Control
MAM      Mobile Application Management
MAN      Metropolitan Area Network
MBR      Master Boot Record
MD5      Message Digest 5
MDF      Main Distribution Frame
MDM      Mobile Device Management
MDM      Mobile Application Management
MDM      Mobile Device Management
MFA      Multifactor Authentication
MFD      Multifunction Device
MFP      Multifunction Printer
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MITM</td>
<td>Man-in-the-Middle</td>
</tr>
<tr>
<td>ML</td>
<td>Machine Learning</td>
</tr>
<tr>
<td>MMS</td>
<td>Multimedia Message Service</td>
</tr>
<tr>
<td>MOA</td>
<td>Memorandum of Agreement</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>MSA</td>
<td>Measurement Systems Analysis</td>
</tr>
<tr>
<td>MSCHAP</td>
<td>Microsoft Challenge Handshake Authentication</td>
</tr>
<tr>
<td>MSP</td>
<td>Managed Service Provider</td>
</tr>
<tr>
<td>MSSP</td>
<td>Managed Security 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 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>NAS</td>
<td>Network-attached Storage</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>NFV</td>
<td>Network Function Virtualization</td>
</tr>
<tr>
<td>NGFW</td>
<td>Next-generation Firewall</td>
</tr>
<tr>
<td>NG-SWG</td>
<td>Next-generation Secure Web Gateway</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</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>NOC</td>
<td>Network Operations Center</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 Authentication</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>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>OSINT</td>
<td>Open-source Intelligence</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
<tr>
<td>OTA</td>
<td>Over-The-Air</td>
</tr>
<tr>
<td>OTG</td>
<td>On-The-Go</td>
</tr>
<tr>
<td>OVAL</td>
<td>Open Vulnerability and Assessment Language</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</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>Privileged Access Management</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>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PDU</td>
<td>Power Distribution Unit</td>
</tr>
<tr>
<td>PE</td>
<td>Portable Executable</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>PED</td>
<td>Portable Electronic Device</td>
</tr>
<tr>
<td>PEM</td>
<td>Privacy Enhanced Mail</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</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>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification</td>
</tr>
<tr>
<td>PKC</td>
<td>Public Key Cryptography Standards</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PoC</td>
<td>Proof of Concept</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>PUP</td>
<td>Potentially Unwanted Program</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</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 Service</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Inexpensive Disks</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Server</td>
</tr>
<tr>
<td>RAT</td>
<td>Remote Access Trojan</td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher version 4</td>
</tr>
<tr>
<td>RCS</td>
<td>Rich Communication Services</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</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>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>SAE</td>
<td>Simultaneous Authentication of Equals</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertions Markup Language</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory 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>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 Networking</td>
</tr>
<tr>
<td>SDP</td>
<td>Service Delivery Platform</td>
</tr>
<tr>
<td>SDV</td>
<td>Software-defined Visibility</td>
</tr>
<tr>
<td>SED</td>
<td>Self-Encrypting Drives</td>
</tr>
<tr>
<td>SEH</td>
<td>Structured Exception Handling</td>
</tr>
<tr>
<td>SFTP</td>
<td>SSH File Transfer Protocol</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
</tr>
<tr>
<td>S-HTTP</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>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>S/MIME</td>
<td>Secure/Multipurpose Internet Mail Extensions</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>SOAR</td>
<td>Security Orchestration, Automation, Response</td>
</tr>
<tr>
<td>SoC</td>
<td>System on Chip</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Center</td>
</tr>
<tr>
<td>SP</td>
<td>Sender Policy Framework</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>SQLi</td>
<td>SQL Injection</td>
</tr>
<tr>
<td>SRTP</td>
<td>Secure Real-time Transport 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>STIX</td>
<td>Structured Threat Information eXpression</td>
</tr>
<tr>
<td>STP</td>
<td>Shielded Twisted Pair</td>
</tr>
<tr>
<td>SWG</td>
<td>Secure Web Gateway</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System</td>
</tr>
<tr>
<td>TAXII</td>
<td>Trusted Automated eXchange of Indicator Information</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></td>
<td></td>
</tr>
<tr>
<td></td>
<td></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>TTP</td>
<td>Tactics, Techniques, and Procedures</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>UEBA</td>
<td>User and Entity Behavior Analytics</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
<tr>
<td>UEM</td>
<td>Unified Endpoint Management</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>USMOTG</td>
<td>USB On-The-Go</td>
</tr>
<tr>
<td>UTM</td>
<td>Unified Threat Management</td>
</tr>
<tr>
<td>UTP</td>
<td>Unshielded Twisted Pair</td>
</tr>
<tr>
<td>VBA</td>
<td>Visual Basic</td>
</tr>
<tr>
<td>VDE</td>
<td>Virtual Desktop Environment</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual 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>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Private Cloud</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>WORM</td>
<td>Write Once Read Many</td>
</tr>
<tr>
<td>WPA</td>
<td>WiFi Protected Access</td>
</tr>
<tr>
<td>WPS</td>
<td>WiFi Protected Setup</td>
</tr>
<tr>
<td>WTLS</td>
<td>Wireless TLS</td>
</tr>
<tr>
<td>XaaS</td>
<td>Anything as a Service</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive Or</td>
</tr>
<tr>
<td>XSS</td>
<td>Cross-site Scripting</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 are not exhaustive.

HARDWARE
• Laptop with Internet access
• Separate wireless NIC
• WAP
• Firewall
• UTM
• Mobile device
• Server/cloud server
• IoT devices

SOFTWARE
• Virtualization software
• Penetration testing OS/distributions (e.g., Kali Linux, ParrotOS)
• SIEM
• Wireshark
• Metasploit
• tcpdump

OTHER
• Access to a CSP