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 instant 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
- Typosquatting
- 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 table
  - 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
| Given a scenario, analyze potential indicators associated with application attacks. |
| --- | --- | --- |
| • Privilege escalation | • Race conditions | • Application programming interface (API) attacks |
| • Cross-site scripting | • Time of check/time of use | • Resource exhaustion |
| • Injections | • Error handling | • Memory leak |
|  - Structured query language (SQL) | • Improper input handling | • Secure Sockets Layer (SSL) stripping |
|  - Dynamic-link library (DLL) | • Replay attack | • Driver manipulation |
|  - Lightweight Directory Access Protocol (LDAP) |  - Session replays |  - Shimming |
|  - Extensible Markup Language (XML) | • Integer overflow |  - Refactoring |
| • Pointer/object dereference | • Request forgeries | • Pass the hash |
| • Directory traversal |  - Server-side | |
| • Buffer overflows |  - Cross-site | |

| Given a scenario, analyze potential indicators associated with network attacks. |
| --- | --- | --- |
| • Wireless | • Layer 2 attacks | • Application |
|  - Evil twin |  - Address Resolution |  - Operational technology (OT) |
|  - Rogue access point |  - Protocol (ARP) poisoning |  - Malicious code or script execution |
|  - Bluesnarfing |  - Media access control (MAC) flooding |  - PowerShell |
|  - Bluejacking |  - MAC cloning |  - Python |
|  - Disassociation |  - Domain hijacking |  - Bash |
|  - Jamming |  - DNS poisoning |  - Macros |
|  - Radio frequency identification (RFID) |  - Uniform Resource Locator (URL) redirection |  - Visual Basic for Applications (VBA) |
|  - Near-field communication (NFC) |  - Domain reputation | |
|  - Initialization vector (IV) |  - Network | |
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
    - Authorized
    - Unauthorized
    - Semi-authorized
  - 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

- **Automated Indicator Sharing (AIS)**
- **Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII)**
- **Predictive analysis**
- **Threat maps**
- **File/code repositories**

- **Research sources**
  - Vendor websites
  - Vulnerability feeds
  - Conferences
  - Academic journals
  - Request for comments (RFC)
  - Local industry groups
  - Social media
  - Threat feeds
  - Adversary tactics, techniques, and procedures (TTP)
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
  - Credentialed vs. non-credentialed
  - 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**
  - Known environment
  - Unknown environment
  - Partially known environment
  - Rules of engagement
  - Lateral movement
  - Privilege escalation
  - Persistence
  - Cleanup
  - Bug bounty
  - Pivoting

- **Passive and active reconnaissance**
  - Drones
  - 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
- Geographical considerations
- 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
- Cloud service providers
- 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.

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

### 2.4 Summarize authentication and authorization design concepts.

<table>
<thead>
<tr>
<th>Authentication methods</th>
<th>Biometrics</th>
<th>Multifactor authentication (MFA) factors and attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Directory services</td>
<td>- Fingerprint</td>
<td>- Factors</td>
</tr>
<tr>
<td>- Federation</td>
<td>- Retina</td>
<td>- Something you know</td>
</tr>
<tr>
<td>- Attestation</td>
<td>- Iris</td>
<td>- Something you have</td>
</tr>
<tr>
<td>- Technologies</td>
<td>- Facial</td>
<td>- Something you are</td>
</tr>
<tr>
<td>- Time-based one-time password (TOTP)</td>
<td>- Voice</td>
<td>- Attributes</td>
</tr>
<tr>
<td>- HMAC-based one-time password (HOTP)</td>
<td>- Vein</td>
<td>- Somewhere you are</td>
</tr>
<tr>
<td>- Short message service (SMS)</td>
<td>- Gait analysis</td>
<td>- Something you can do</td>
</tr>
<tr>
<td>- Token key</td>
<td>- Efficacy rates</td>
<td>- Something you exhibit</td>
</tr>
<tr>
<td>- Static codes</td>
<td>- False acceptance</td>
<td>- Someone you know</td>
</tr>
<tr>
<td>- Authentication applications</td>
<td>- False rejection</td>
<td></td>
</tr>
<tr>
<td>- Push notifications</td>
<td>- Crossover error rate</td>
<td></td>
</tr>
<tr>
<td>- Phone call</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Smart card authentication</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

- 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
- Access control vestibules
- 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
  - USB data blocker
- Lighting
- Fencing
- Fire suppression
- Sensors
  - Motion detection
  - Noise detection
  - Proximity reader
  - Moisture detection
  - Cards
  - Temperature
- Drones
- Visitor logs
- Faraday cages
- Air gap
- Screened subnet (previously known as demilitarized zone)
- 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
- Supporting integrity
- Supporting obfuscation
- Supporting authentication
- Supporting non-repudiation
- 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 Extensions (DNSSEC)
  - SSH
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Secure Real-time Transport Protocol (SRTP)
  - Lightweight Directory Access Protocol Over SSL (LDAPS)
  - File Transfer Protocol, Secure (FTPS)
  - SSH File Transfer Protocol (SFTP)
- **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
  - Boot attestation
- **Database**
  - Tokenization
  - Salting
  - Hashing
- **Application security**
  - Input validations
  - Secure cookies
  - Hypertext Transfer Protocol (HTTP) headers
  - Code signing
  - Allow list
  - Block list/deny list
  - Secure coding practices
  - Static code analysis
    - Manual code review
    - Dynamic code analysis
    - Fuzzing
- **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)
  - Screened subnet (previously known as demilitarized zone)
  - 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
  - Collectors

Given a scenario, install and configure wireless security settings.

- **Cryptographic protocols**
  - WiFi Protected Access 2 (WPA2)
  - WiFi Protected Access 3 (WPA3)
  - Counter-mode/CBC-MAC Protocol (CCMP)
  - Simultaneous Authentication of Equals (SAE)

- **Authentication protocols**
  - Extensible Authentication Protocol (EAP)
  - Protected Extensible Authentication 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 overlaps
  - Wireless access point (WAP) placement

- 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

- **Controller and access point security**
3.0 Implementation

3.5 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 device management (MDM)**
  - Application management
  - Content management
  - Remote wipe
  - Geo-fencing
  - Geolocation
  - Screen locks
  - Push notifications
  - Passwords and PINs
  - Biometrics
  - Context-aware authentication
  - Containerization
  - Storage segmentation
  - Full device encryption

- **Mobile devices**
  - MicroSD hardware
  - Security module (HSM)
  - MDM/Unified Endpoint Management (UEM)
  - Mobile application management (MAM)
  - SEAndroid

- **Enforcement and monitoring of:**
  - Third-party application stores
  - Rooting/jailbreaking
  - Sideload
  - Custom firmware
  - Carrier unlocking
  - Firmware over-the-air (OTA) updates

- **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
  - Password reuse
  - Network location
  - Geofencing
  - Geotagging
  - Geolocation
  - Time-based logins
- **Account types**
  - User account
  - Shared and generic accounts/credentials
  - Guest accounts
  - Service accounts
  - Access policies
  - Account permissions
  - Account audits
  - Impossible travel time/risky login
  - Lockout
  - Disablement

3.8 Given a scenario, implement authentication and authorization solutions.

- **Authentication management**
  - Password keys
  - Password vaults
  - TPM
  - HSM
  - Knowledge-based authentication
- **Authentication/authorization**
  - EAP
  - Challenge-Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)
  - 802.1X
  - RADIUS
  - Single sign-on (SSO)
  - Security Assertion Markup Language (SAML)
  - Terminal Access Controller Access Control System Plus (TACACS+)
  - OAuth
  - OpenID
  - Kerberos
- **Access control schemes**
  - Attribute-based access control (ABAC)
  - Role-based access control
  - Rule-based access control
  - MAC
  - Discretionary access control (DAC)
  - Conditional access
  - Privileged 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)
  - Privacy enhanced mail (PEM)
  - Personal information exchange (PFX)
  - .cer
  - .p12
  - .p7b
- **Concepts**
  - Online vs. offline CA
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining
### 4.0 Operations and Incident Response

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

<table>
<thead>
<tr>
<th>Network reconnaissance and discovery</th>
<th>Shell and script environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>- tracert/traceroute</td>
<td>- scanless</td>
</tr>
<tr>
<td>- nslookup/dig</td>
<td>- head</td>
</tr>
<tr>
<td>- ipconfig/icmpconfig</td>
<td>- tail</td>
</tr>
<tr>
<td>- nmap</td>
<td>- cat</td>
</tr>
<tr>
<td>- ping/ PATHping</td>
<td>- grep</td>
</tr>
<tr>
<td>- hping</td>
<td>- chmod</td>
</tr>
<tr>
<td>- netstat</td>
<td>- logger</td>
</tr>
<tr>
<td>- netcat</td>
<td></td>
</tr>
<tr>
<td>- IP scanners</td>
<td></td>
</tr>
<tr>
<td>- arp</td>
<td></td>
</tr>
<tr>
<td>- route</td>
<td></td>
</tr>
<tr>
<td>- curl</td>
<td></td>
</tr>
<tr>
<td>- theHarvester</td>
<td></td>
</tr>
<tr>
<td>- sn1per</td>
<td></td>
</tr>
</tbody>
</table>

- OpenSSL
- Packet capture and replay
- Tcppreplay
- Tcpcap
- 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
4.3 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
- SIEM dashboards
  - Sensor
  - Sensitivity
  - Trends
  - Alerts
  - Correlation
  - Alerts
- Log files
  - Network
  - System
  - Application
- Vulnerability scan output

- Security
- Web
- DNS
- Authentication
- Dump files
- VoIP and call managers
- Session Initiation Protocol (SIP) traffic
  - syslog/rsyslog/syslog-ng
  - journalctl
  - NXLog
  - Bandwidth monitors
- Metadata
  - Email
  - Mobile
  - Web
  - File
- Netflow/sFlow
  - Netflow
  - sFlow
  - IPFIX
  - Protocol analyzer output

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

- Reconfigure endpoint security solutions
  - Application approved list
  - Application blocklist/deny list
  - 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**
  - Preventive
  - 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) Risk Management Framework (RMF)/Cybersecurity Framework (CSF)
  - International Organization for Standardization (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Type I/II
  - Cloud security alliance

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

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

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

- **Organizational policies**
  - Change management
  - Change control
  - Asset management

CompTIA Security+ Certification Exam Objectives Version 3.0 (Exam Number: SY0-601)
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
  - Risk control self-assessment
  - Risk awareness
  - Inherent risk
  - Residual risk
  - Control risk
  - Risk appetite
  - Regulations that affect risk posture
  - Risk assessment types
    - Qualitative
    - Quantitative
  - Likelihood of occurrence
  - Impact
  - Asset value
  - Single-loss expectancy (SLE)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
- **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

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

- **Organizational consequences of privacy and data 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)
- **Information life cycle**
- **Impact assessment**
- **Terms of agreement**
- **Privacy notice**
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>
<th>ACRONYM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DER</td>
<td>Distinguished Encoding Rules</td>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
<td>HSMAas</td>
<td>Hardware Security Module as a Service</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
<td>HTML</td>
<td>Hypertext Markup Language</td>
</tr>
<tr>
<td>DHE</td>
<td>Diffie-Hellman Ephemeral</td>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>DKIM</td>
<td>Domain Keys Identified Mail</td>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>DLL</td>
<td>Dynamic-link Library</td>
<td>HVAC</td>
<td>Heating, Ventilation, Air Conditioning</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>DMARC</td>
<td>Domain Message Authentication</td>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>Domain Name System Security</td>
<td>ICS</td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial-of-Service</td>
<td>IDEA</td>
<td>International Data Encryption Algorithm</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
<td>ICV</td>
<td>Incident Response</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
<td>IPsec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
<td>IR</td>
<td>Incident Response Plan</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
<td>IOC</td>
<td>Indicators of Compromise</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Code Book</td>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic-curve Cryptography</td>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ECDHE</td>
<td>Elliptic-curve Diffie-Hellman Ephemeral</td>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic-curve Digital Signature Algorithm</td>
<td>IR</td>
<td>Incident Response Plan</td>
</tr>
<tr>
<td>EDR</td>
<td>Endpoint Detection and Response</td>
<td>IRC</td>
<td>Internet Relay Chat</td>
</tr>
<tr>
<td>EFS</td>
<td>Encrypted File System</td>
<td>IRP</td>
<td>Incident Response Plan</td>
</tr>
<tr>
<td>EIP</td>
<td>Extended Instruction Pointer</td>
<td>ISA</td>
<td>Interconnection Security Agreement</td>
</tr>
<tr>
<td>EOL</td>
<td>End of Life</td>
<td>ISFW</td>
<td>Internal Segmentation Firewall</td>
</tr>
<tr>
<td>EOS</td>
<td>End of Service</td>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
<td>ISSO</td>
<td>Information Systems Security Officer</td>
</tr>
<tr>
<td>ESN</td>
<td>Electronic Serial Number</td>
<td>ITCP</td>
<td>IT Contingency Plan</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>ESSID</td>
<td>Extended Service Set Identifier</td>
<td>KDC</td>
<td>Key Distribution Center</td>
</tr>
<tr>
<td>FACIL</td>
<td>File System Access Control List</td>
<td>KEK</td>
<td>Key Encryption Key</td>
</tr>
<tr>
<td>FDE</td>
<td>Full Disk Encryption</td>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>FIM</td>
<td>File Integrity Monitoring</td>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable Gate Array</td>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>FRR</td>
<td>False Rejection Rate</td>
<td>LEAP</td>
<td>Lightweight Extensible Authentication Protocol</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>MaaS</td>
<td>Monitoring as a Service</td>
</tr>
<tr>
<td>FTPS</td>
<td>Secure File Transfer Protocol</td>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>GCM</td>
<td>Galois/Counter Mode</td>
<td>MAM</td>
<td>Mobile Application Management</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>GPG</td>
<td>GNU Privacy Guard</td>
<td>MBR</td>
<td>Master Boot Record</td>
</tr>
<tr>
<td>GPO</td>
<td>Group Policy Object</td>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
<td>MDF</td>
<td>Main Distribution Frame</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</td>
<td>MDM</td>
<td>Mobile Device Management</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
<td>MFA</td>
<td>Multifactor Authentication</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
<td>MFD</td>
<td>Multifunction Device</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
<td>MFP</td>
<td>Multifunction Printer</td>
</tr>
<tr>
<td>HID</td>
<td>Host-based Intrusion Detection System</td>
<td>MHP</td>
<td>Machine Learning</td>
</tr>
<tr>
<td>HIPS</td>
<td>Host-based Intrusion Prevention System</td>
<td>MHP</td>
<td>Machine Learning</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hash-based Message Authentication Code</td>
<td>ML</td>
<td>Machine Learning</td>
</tr>
<tr>
<td>HOTP</td>
<td>HMAC-based One-time Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACRONYM</td>
<td>DEFINITION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MMS</td>
<td>Multimedia Message Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOA</td>
<td>Memorandum of Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSA</td>
<td>Measurement Systems Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS-CHAP</td>
<td>Microsoft Challenge-Handshake Authentication Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSP</td>
<td>Managed Service Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSSP</td>
<td>Managed Security Service Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time to Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time to Repair</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS</td>
<td>Network-attached Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDA</td>
<td>Non-disclosure Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFC</td>
<td>Near-field Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFV</td>
<td>Network Function Virtualization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGFW</td>
<td>Next-generation Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NG-SWG</td>
<td>Next-generation Secure Web Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIDS</td>
<td>Network-based Intrusion Detection System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIPS</td>
<td>Network-based Intrusion Prevention System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards &amp; Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTLN</td>
<td>New Technology LAN Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Status Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSINT</td>
<td>Open-source Intelligence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTA</td>
<td>Over-The-Air</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTG</td>
<td>On-The-Go</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OVAL</td>
<td>Open Vulnerability and Assessment Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P12</td>
<td>PKCS #12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-Peer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAC</td>
<td>Proxy Auto Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAM</td>
<td>Privileged Access Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAM</td>
<td>Pluggable Authentication Modules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PBKDF2</td>
<td>Password-based Key Derivation Function 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PBX</td>
<td>Private Branch Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCAP</td>
<td>Packet Capture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDU</td>
<td>Power Distribution Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE</td>
<td>Portable Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PED</td>
<td>Portable Electronic Device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PEM</td>
<td>Privacy Enhanced Mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKCS</td>
<td>Public Key Cryptography Standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PoC</td>
<td>Proof of Concept</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP</td>
<td>Post Office Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POTS</td>
<td>Plain Old Telephone Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSK</td>
<td>Preshared Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ</td>
<td>Pan-Tilt-Zoom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PUP</td>
<td>Potentially Unwanted Program</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAD</td>
<td>Rapid Application Development</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-in User Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Inexpensive Disks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAT</td>
<td>Remote Access Trojan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher version 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RCS</td>
<td>Rich Communication Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIPEMD</td>
<td>RACE Integrity Primitives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ROI</td>
<td>Return on Investment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, &amp; Adleman</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTBH</td>
<td>Remotely Triggered Black Hole</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTOS</td>
<td>Real-time Operating System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTP</td>
<td>Real-time Transport Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure/Multipurpose Internet Mail Extensions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAE</td>
<td>Simultaneous Authentication of Equals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertions Markup Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCAP</td>
<td>Security Content Automation Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACRONYM</td>
<td>DEFINITION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCEP</td>
<td>Simple Certificate Enrollment Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDLM</td>
<td>Software Development Life-cycle Methodology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDN</td>
<td>Software-defined Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDP</td>
<td>Service Delivery Platform</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDV</td>
<td>Software-defined Visibility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEH</td>
<td>Structured Exception Handling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFTP</td>
<td>SSH File Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLA</td>
<td>Service-level Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLE</td>
<td>Single Loss Expectancy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB</td>
<td>Server Message Block</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure/Multipurpose Internet Mail Extensions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTPS</td>
<td>Simple Mail Transfer Protocol Secure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOAR</td>
<td>Security Orchestration, Automation, Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SoC</td>
<td>System on Chip</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPF</td>
<td>Sender Policy Framework</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPIM</td>
<td>Spam over Instant Messaging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQLi</td>
<td>SQL Injection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRTP</td>
<td>Secure Real-time Transport Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STIX</td>
<td>Structured Threat Information eXpression</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STP</td>
<td>Shielded Twisted Pair</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWG</td>
<td>Secure Web Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAXII</td>
<td>Trusted Automated eXchange of Intelligence Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TGT</td>
<td>Ticket Granting Ticket</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTP</td>
<td>Time-based One Time Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TSIG</td>
<td>Transaction Signature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTP</td>
<td>Tactics, Techniques, and Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAT</td>
<td>User Acceptance Testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UEBA</td>
<td>User and Entity Behavior Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UEM</td>
<td>Unified Endpoint Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Uniform Resource Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USB OTG</td>
<td>USB On-The-Go</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTM</td>
<td>Unified Threat Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTP</td>
<td>Unshielded Twisted Pair</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VBA</td>
<td>Visual Basic for Applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VDE</td>
<td>Virtual Desktop Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLSM</td>
<td>Variable-length Subnet Masking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Private Cloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VTC</td>
<td>Video Teleconferencing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Access Point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WIDS</td>
<td>Wireless Intrusion Detection System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WIPS</td>
<td>Wireless Intrusion Prevention System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WORM</td>
<td>Write Once Read Many</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPA</td>
<td>WiFi Protected Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPS</td>
<td>WiFi Protected Setup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XaaS</td>
<td>Anything as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive OR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XSS</td>
<td>Cross-site Scripting</td>
<td></td>
<td></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 for 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, Parrot OS)
- SIEM
- Wireshark
- Metasploit
- tcpdump

**OTHER**
- Access to a CSP