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 | Pharming | Tailgating | Eliciting information | Whaling | Prepending | Identity fraud | Invoice scams | Credential harvesting | Reconnaissance | Hoax | Impersonation | Watering hole attack | Typo squatting | 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.

<table>
<thead>
<tr>
<th>Malware</th>
<th>Password attacks</th>
<th>Physical attacks</th>
<th>Adversarial artificial intelligence (AI)</th>
<th>Supply-chain attacks</th>
<th>Cryptographic attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>Spraying</td>
<td>Malicious universal</td>
<td>Tainted training data for machine learning (ML)</td>
<td>Cloud-based vs. on-premises attacks</td>
<td>Birthday</td>
</tr>
<tr>
<td>Trojans</td>
<td>Dictionary</td>
<td>serial bus (USB) cable</td>
<td>Security of machine learning algorithms</td>
<td></td>
<td>Collision</td>
</tr>
<tr>
<td>Worms</td>
<td>Brute force</td>
<td>Malicious flash drive</td>
<td></td>
<td></td>
<td>Downgrade</td>
</tr>
<tr>
<td>Potentially unwanted programs (PUPs)</td>
<td>Offline</td>
<td>Card cloning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fileless virus</td>
<td>Online</td>
<td>Skimming</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command and control</td>
<td>Rainbow tables</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bots</td>
<td>Plaintext/unencrypted</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

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
- 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
- Man in the browser
- Distributed denial of service (DDoS)
  - Network
  - Application
  - Operational technology (OT)
- Malicious code or script execution
  - PowerShell
  - Python
  - Bash
  - Macros
  - Virtual Basic for Applications (VBA)
  - Domain reputation
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

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

- **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

- **Actors and threats**
  - Automated indicator sharing (AIS)
  - Structured threat information exchange (STIX)/Trusted automated exchange of indicator 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)

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

- **Cloud-based vs. on-premises vulnerabilities**
- **Zero-day**
- **Weak configurations**
  - Open permissions
  - Unsecured 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
  - 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, 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**
- **Micro-services/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
### 2.5 Given a scenario, implement cybersecurity resilience.

<table>
<thead>
<tr>
<th>Redundancy</th>
<th>Replication</th>
<th>Non-persistence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographic dispersal</td>
<td>- Storage area network (SAN)</td>
<td>- Revert to known state</td>
</tr>
<tr>
<td>Disk</td>
<td>- VM</td>
<td>- Last known good config</td>
</tr>
<tr>
<td>RAID levels</td>
<td>- On-premises vs. cloud</td>
<td>- Live boot media</td>
</tr>
<tr>
<td>Multipath</td>
<td>- Full</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>- Incremental</td>
<td>High availability</td>
</tr>
<tr>
<td>Load balancers</td>
<td>- Snapshot</td>
<td>- Scalability</td>
</tr>
<tr>
<td>Network interface</td>
<td>- Differential</td>
<td></td>
</tr>
<tr>
<td>NIC teaming</td>
<td>- Tape</td>
<td></td>
</tr>
<tr>
<td>Power</td>
<td>- Disk</td>
<td></td>
</tr>
<tr>
<td>UPS</td>
<td>- Copy</td>
<td></td>
</tr>
<tr>
<td>Generator</td>
<td>- Network attached storage (NAS)</td>
<td></td>
</tr>
<tr>
<td>Dual supply</td>
<td>- SAN</td>
<td></td>
</tr>
<tr>
<td>Managed power</td>
<td>- Cloud</td>
<td></td>
</tr>
<tr>
<td>distribution units</td>
<td>- Image</td>
<td></td>
</tr>
<tr>
<td>(PDUs)</td>
<td>- Online vs. offline</td>
<td></td>
</tr>
</tbody>
</table>

### 2.6 Explain the security implications of embedded and specialized systems.

<table>
<thead>
<tr>
<th>Embedded systems</th>
<th>Specialized</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raspberry Pi</td>
<td>- Medical systems</td>
<td>- Subscriber identity module (SIM) cards</td>
</tr>
<tr>
<td>Field programmable gate array (FPGA)</td>
<td>- Vehicles</td>
<td>- Power</td>
</tr>
<tr>
<td>Arduino</td>
<td>- Aircraft</td>
<td>- Compute</td>
</tr>
<tr>
<td>System control and data acquisition (SCADA)/industrial control system (ICS)</td>
<td>- Smart meters</td>
<td>- Network</td>
</tr>
<tr>
<td>Facilities</td>
<td>- Voice over IP (VoIP)</td>
<td>- Crypto</td>
</tr>
<tr>
<td>Industrial</td>
<td>- Heating, ventilation, air conditioning (HVAC)</td>
<td>- Inability to patch</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>- Drones/AVs</td>
<td>- Authentication</td>
</tr>
<tr>
<td>Energy</td>
<td>- Multifunction printer (MFP)</td>
<td>- Range</td>
</tr>
<tr>
<td>Logistics</td>
<td>- Real-time operating system (RTOS)</td>
<td>- Cost</td>
</tr>
<tr>
<td>Internet of Things (IoT)</td>
<td>- Surveillance systems</td>
<td>- Implied trust</td>
</tr>
<tr>
<td>Sensors</td>
<td>- System on chip (SoC)</td>
<td></td>
</tr>
<tr>
<td>Smart devices</td>
<td>- Communication considerations</td>
<td></td>
</tr>
<tr>
<td>Wearables</td>
<td>- 5G</td>
<td></td>
</tr>
<tr>
<td>Facility automation</td>
<td>- Narrow-band</td>
<td></td>
</tr>
<tr>
<td>Weak defaults</td>
<td>- Baseband radio</td>
<td></td>
</tr>
</tbody>
</table>
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
  - USB data blocker
- Lightning
- 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
  - USB data blocker
- Lightning
- 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
- Elliptical 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
  - 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 exchanger (S/MIME)
  - Secure real-time protocol (SRTP)
  - LDAPS
  - File transfer protocol, secure (FTPS)
  - Secured file transfer protocol (SFTP)
  - Simple Network Management Protocol, version 3 (SNMPv3)
  - Hypertext transfer protocol over SSL/TLS (HTTPS)
  - IPSec
    - Authentication header (AH)/Encapsulated security payload (ESP)
    - Tunnel/transport
  - Secure post office protocol (POP)/Internet message access protocol (IMAP)

- Use cases
  - Voice and video
  - Time synchronization

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
  - Host intrusion prevention system (HIPS)
  - Host 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

- 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

CompTIA Security+ Certification Exam Objectives Version 1.0 (Exam Number: SY0-601)
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

- **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 Server (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

- **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**

---

CompTIA Security+ Certification Exam Objectives Version 1.0 (Exam Number: SY0-601)
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 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

- **Mobile devices**
  - Microsoft HSM
  - MDM/Unified endpoint management (UEM)
  - Mobile application management (MAM)
  - SEAndroid

- **Enforcement and monitoring of**
  - Third-party app stores
  - Rooting/jailbreaking
  - Sideloading
  - Custom firmware
  - Carrier unlocking
  - Firmware over-the-air (OTA) updates
  - Camera use

- **Deployment models**
  - Bring your own device (BYOD)
  - Corporate-owned personally enabled (COPE)
  - Choose your own device (CYOD)
  - Corporate-owned
  - Virtual desktop infrastructure (VDI)

- **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**
3.7 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
  - Time of day
  - Network location
  - Geofencing
  - Geotagging
  - Geolocation
- **Account types**
  - User account
  - Shared and generic accounts/credentials
  - Guest accounts
  - Service accounts
- **Authentication management**
  - Password keys
  - Password vaults
  - TPM
  - HSM
  - Knowledge-based authentication
  - EAP
  - Challenge Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)
  - 802.1X
  - RADIUS
  - Single sign-on (SSO)
  - Security Assertions Markup Language (SAML)
  - Terminal Access Controller Access Control System Plus (TACACS+)
  - OAuth
  - OpenID
  - Kerberos
- **Access control schemes**
  - Attribute-based access control (ABAC)

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
  - SAN
  - Expiration
- **Types of certificates**
  - Wildcard
  - SAN
  - 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>File manipulation</th>
<th>Shell and script environments</th>
<th>Forensics</th>
<th>Exploitation frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>- tracert/traceroute</td>
<td>- head</td>
<td>- SSH</td>
<td>- dd</td>
<td>- Packet capture and replay</td>
</tr>
<tr>
<td>- nslookup/dig</td>
<td>- tail</td>
<td>- PowerShell</td>
<td>- Memdump</td>
<td>- Tcpreplay</td>
</tr>
<tr>
<td>- ipconfig/ifconfig</td>
<td>- cat</td>
<td>- Python</td>
<td>- WinHex</td>
<td>- Tcpdump</td>
</tr>
<tr>
<td>- nmap</td>
<td>- grep</td>
<td></td>
<td>- FTK imager</td>
<td>- Wireshark</td>
</tr>
<tr>
<td>- ping/pathping</td>
<td>- chmod</td>
<td></td>
<td>- Autopsy</td>
<td></td>
</tr>
<tr>
<td>- hping</td>
<td>- logger</td>
<td></td>
<td></td>
<td>- Exploitation frameworks</td>
</tr>
<tr>
<td>- netstat</td>
<td></td>
<td></td>
<td></td>
<td>- Password crackers</td>
</tr>
<tr>
<td>- netcat</td>
<td></td>
<td></td>
<td></td>
<td>- Data sanitization</td>
</tr>
<tr>
<td>- IP scanners</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- arp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- route</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- curl</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- the harvester</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- sn1per</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Incident response plans</th>
<th>Exercises</th>
<th>Stakeholder management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident response process</td>
<td>- Tabletop</td>
<td>- Communication plan</td>
</tr>
<tr>
<td>- Preparation</td>
<td>- Walkthroughs</td>
<td>- Disaster recovery plan</td>
</tr>
<tr>
<td>- Identification</td>
<td>- Simulations</td>
<td>- Business continuity plan</td>
</tr>
<tr>
<td>- Containment</td>
<td>- Attack frameworks</td>
<td>- Continuity of operation planning (COOP)</td>
</tr>
<tr>
<td>- Eradication</td>
<td>- MITRE ATT&amp;CK</td>
<td>- Incident response team</td>
</tr>
<tr>
<td>- Recovery</td>
<td>- The Diamond Model of Intrusion Analysis</td>
<td>- Retention policies</td>
</tr>
<tr>
<td>- Lessons learned</td>
<td>- Cyber Kill Chain</td>
<td></td>
</tr>
</tbody>
</table>

CompTIA Security+ Certification Exam Objectives Version 1.0 (Exam Number: SY0-601)
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
- nlog
- 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
- Secure Orchestration, Automation, and Response (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
  - SSAE SOC 2 Type II/III
  - Cloud security alliance
  - Cloud control matrix
  - Reference architecture

- **Benchmarks / secure configuration guides**
  - 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

- **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 1.0 (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)

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

- **Disasters**
  - Environmental
  - Man-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

- **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
  - Information life cycle
  - Impact assessment
  - Terms of agreement
  - Privacy notice

- **Privacy enhancing technologies**
  - Data minimization
  - Data masking
  - Tokenization
  - Anonymization
  - Pseudo-anonymization
- **Roles and responsibilities**
  - Data owners
  - Data controller
  - Data processor
  - Data custodian/steward
  - Data privacy officer (DPO)
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>3DES</td>
<td>Triple Digital Encryption Standard</td>
<td>CBC</td>
<td>Cipher Block Chaining</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
<td>CBT</td>
<td>Computer-based Training</td>
</tr>
<tr>
<td>ABAC</td>
<td>Attribute-based Access Control</td>
<td>CCMP</td>
<td>Counter-Mode/CBC-Mac Protocol</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>AES256</td>
<td>Advanced Encryption Standards 256bit</td>
<td>CFB</td>
<td>Cipher Feedback</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>AIS</td>
<td>Automated Indicator Sharing</td>
<td>CIRT</td>
<td>Computer Incident Response Team</td>
</tr>
<tr>
<td>ALE</td>
<td>Annualized Loss Expectancy</td>
<td>CIS</td>
<td>Center for Internet Security</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td>CMS</td>
<td>Content Management System</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
<td>COOP</td>
<td>Continuity of Operation Planning</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
<td>COPE</td>
<td>Corporate Owned Personal Enabled</td>
</tr>
<tr>
<td>ARO</td>
<td>Annualized Rate of Occurrence</td>
<td>CP</td>
<td>Contingency Planning</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
<td>CRC</td>
<td>Cyclical Redundancy Check</td>
</tr>
<tr>
<td>ASLR</td>
<td>Address Space Layout Randomization</td>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>ASP</td>
<td>Active Server Page</td>
<td>CSO</td>
<td>Chief Security Officer</td>
</tr>
<tr>
<td>ATT&amp;CK</td>
<td>Adversarial Tactics, Techniques, and Common Knowledge</td>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
<td>CSR</td>
<td>Certificate Signing Request</td>
</tr>
<tr>
<td>AV</td>
<td>Antivirus</td>
<td>CSRF</td>
<td>Cross-Site Request Forgery</td>
</tr>
<tr>
<td>BASH</td>
<td>Bourne Again Shell</td>
<td>CTO</td>
<td>Chief Technology Officer</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Planning</td>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
<td>CVSS</td>
<td>Common Vulnerability Scoring System</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
<td>CYOD</td>
<td>Choose Your Own Device</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>BPA</td>
<td>Business Partnership Agreement</td>
<td>DBA</td>
<td>Database Administrator</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
<td>DEP</td>
<td>Data Execution Prevention</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
<td>DER</td>
<td>Distinguished Encoding Rules</td>
</tr>
<tr>
<td>CAC</td>
<td>Common Access Card</td>
<td>DES</td>
<td>Digital Encryption Standard</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>Completely Automated Public Turing Test to Tell Computers and Humans Apart</td>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>CAR</td>
<td>Corrective Action Report</td>
<td>DHE</td>
<td>Diffie-Hellman Ephemeral</td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</td>
<td>DKIM</td>
<td>Domain Keys Identified Mail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DLL</td>
<td>Dynamic Link Library</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>DLP</td>
<td>Data Loss Prevention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMARC</td>
<td>Domain Message Authentication Reporting and Conformance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNAT</td>
<td>Destination Network Address Transaction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service (Server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNSSEC</td>
<td>Domain Name System Security Extensions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO</td>
<td>Data Privacy Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EBC</td>
<td>Electronic Code Book</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDHE</td>
<td>Elliptic Curve Diffie-Hellman Ephemeral</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic Curve Digital Signature Algorithm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDR</td>
<td>Endpoint Detection and Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EFS</td>
<td>Encrypted File System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EOL</td>
<td>End of Life</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EOS</td>
<td>End of Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESN</td>
<td>Electronic Serial Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulated Security Payload</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FACL</td>
<td>File System Access Control List</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDE</td>
<td>Full Disk Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable Gate Array</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FRR</td>
<td>False Rejection Rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTPS</td>
<td>Secured File Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GCM</td>
<td>Galois Counter Mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPG</td>
<td>Gnu Privacy Guard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPO</td>
<td>Group Policy Object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIDS</td>
<td>Host-Based Intrusion Detection System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPS</td>
<td>Host-Based Intrusion Prevention System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMAC</td>
<td>Hashed Message Authentication Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOTP</td>
<td>HMAC based One Time Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTML</td>
<td>HyperText Markup Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol over SSL/TLS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation, Air Conditioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDEA</td>
<td>International Data Encryption Algorithm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDF</td>
<td>Intermediate Distribution Frame</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IdP</td>
<td>Identity Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP4</td>
<td>Internet Message Access Protocol v4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IoC</td>
<td>Indicators of Compromise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRP</td>
<td>Incident Response Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISSO</td>
<td>Information Systems Security Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITCP</td>
<td>IT Contingency Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KDC</td>
<td>Key Distribution Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KEK</td>
<td>Key Encryption Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEAP</td>
<td>Lightweight Extensible Authentication Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MaaS</td>
<td>Monitoring as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAM</td>
<td>Mobile Application Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MBR</td>
<td>Master Boot Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Frame</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDM</td>
<td>Mobile Device Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFA</td>
<td>Multifactor Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFD</td>
<td>Multi-Function Device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFP</td>
<td>Multi-Function Printer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MITM</td>
<td>Man in the Middle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ML</td>
<td>Machine Learning</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>ACRONYM</td>
<td>DEFINITION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------------</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>Multi-Protocol Label Switching</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSA</td>
<td>Measurement Systems Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSCHAP</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 Recover</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 Functions Virtualization</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>NTFS</td>
<td>New Technology File System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTLM</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>OAuth</td>
<td>Open Authorization</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 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>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PED</td>
<td>Personal 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>PFX</td>
<td>Personal Information Exchange</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>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>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>Pre-Shared Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ</td>
<td>Pan-Tilt-Zoom</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>PUP</td>
<td>Potentially Unwanted Program</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RA</td>
<td>Recovery Agent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RACE</td>
<td>Research and Development in Advanced Communications Technologies in Europe</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 Server</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>RFIID</td>
<td>Radio Frequency Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RACE</td>
<td>RACE Integrity Primitives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIPEMD</td>
<td>Evaluation Message Digest</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>Remote 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>RTS</td>
<td>Real-Time Operating System</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>ACRONYM</td>
<td>DEFINITION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------------</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>SAN</td>
<td>Storage Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAN</td>
<td>Subject Alternative Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCADA</td>
<td>System 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>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>SDV</td>
<td>Software Defined Visibility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SED</td>
<td>Self-Encrypting Drives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEH</td>
<td>Structured Exception Handler</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFTP</td>
<td>Secured 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>SHTTP</td>
<td>Secure Hypertext Transfer Protocol</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>S/MIME</td>
<td>Secure/Multipurpose Internet Mail Exchanger</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 Internet 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 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>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 eXchange</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</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TCP/IP  Transmission Control Protocol/Internet Protocol
TGT      Ticket Granting Ticket
TKIP     Temporal Key Integrity Protocol
TLS      Transport Layer Security
TOTP     Time-based One Time Password
TPM      Trusted Platform Module
TSIG     Transaction Signature
TTP      Tactics, Techniques, and Procedures
UAT      User Acceptance Testing
UAV      Unmanned Aerial Vehicle
UDP      User Datagram Protocol
UEFI     Unified Extensible Firmware Interface
UEM      Unified Endpoint Management
UPS      Uninterruptable Power Supply
URI      Uniform Resource Identifier
URL      Universal Resource Locator
USB      Universal Serial Bus
USB OTG  USB On The Go
UTM      Unified Threat Management
UTP      Unshielded Twisted Pair
VBA      Visual Basic
VDE      Virtual Desktop Environment
VDI      Virtual Desktop Infrastructure
VLAN     Virtual Local Area Network
VLSM     Variable Length Subnet Masking
VM       Virtual Machine
VoIP     Voice over IP
VPC      Virtual Private Cloud
VPN      Virtual Private Network
VTC      Video Teleconferencing
WAF      Web Application Firewall
WAP      Wireless Access Point
WEP      Wired Equivalent Privacy
WIDS     Wireless Intrusion Detection System
WIPS     Wireless Intrusion Prevention System
WORM     Write Once Read Many
WPA      WiFi Protected Access
WPS      WiFi Protected Setup
WTLS     Wireless TLS
XaaS     Anything as a Service
XML      Extensible Markup Language
XOR      Exclusive Or
XSRF     Cross-Site Request Forgery
XSS      Cross-Site Scripting
Security+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Security+ exam. This list may also be helpful for training companies 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