EDUSUM

#1 Online Certification Guide

SY0-501

Security+

A Success Guide to Prepare- CompTIA Security+

edusum.com

Table of Contents

Introduction to SY0-501 Exam on CompTIA Security+

Use this quick start guide to collect all the information about CompTIA Security+ (SY0-501) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the SY0-501 Security+ exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual CompTIA Security Plus certification exam.

The CompTIA Security+ certification is mainly targeted to those candidates who want to build their career in IT Security domain. The CompTIA Security+ exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of CompTIA Security Plus.

CompTIA SY0-501 Certification Details:

Exam Name	CompTIA Security+
Exam Code	SY0-501
Exam Price	$320 (USD)
Duration	90 min
Number of Questions	90
Passing Score	750 / 900
Schedule Exam	CompTIA Marketplace
Sample Questions	CompTIA Security+ Sample Questions
Practice Exam	**CompTIA SY0-501 Certification Practice Exam**

CompTIA SY0-501 Exam Syllabus:

Topic	**Details**
Threats, Attacks and Vulnerabilities 21%	
Given a scenario, analyze indicators of compromise and determine the type of malware.	1. Viruses 2. Crypto-malware 3. Ransomware 4. Worm 5. Trojan 6. Rootkit 7. Keylogger 8. Adware 9. Spyware 10. Bots 11. RAT 12. Logic bomb 13. Backdoor
Compare and contrast types of attacks.	1. Social engineering 1. Phishing 2. Spear phishing 3. Whaling 4. Vishing 5. Tailgating 6. Impersonation 7. Dumpster diving 8. Shoulder surfing 9. Hoax 10. Watering hole attack 11. Principles (reasons for effectiveness) 12. Authority 13. Intimidation 14. Consensus 15. Scarcity 16. Familiarity 17. Trust 18. Urgency 2. Application/service attacks 1. DoS 2. DDoS 3. Man-in-the-middle 4. Buffer overflow 5. Injection 6. Cross-site scripting 7. Cross-site request forgery 8. Privilege escalation 9. ARP poisoning

Topic	Details
	10. Amplification 11. DNS poisoning 12. Domain hijacking 13. Man-in-the-browser 14. Zero day 15. Replay 16. Pass the hash 17. Hijacking and related attacks 18. Clickjacking 19. Session hijacking 20. URL hijacking 21. Typo squatting 22. Driver manipulation 23. Shimming 24. Refactoring 25. MAC spoofing 26. IP spoofing 3. Wireless attacks 1. Replay 2. IV 3. Evil twin 4. Rogue AP 5. Jamming 6. WPS 7. Bluejacking 8. Bluesnarfing 9. RFID 10. NFC 11. Disassociation 4. Cryptographic attacks 1. Birthday 2. Known plain text/cipher text 3. Rainbow tables 4. Dictionary 5. Brute force 6. Online vs. offline 7. Collision 8. Downgrade 9. Replay 10. Weak implementations
Explain threat actor types and attributes.	1. Types of actors 1. Script kiddies

Topic	Details
	2. Hacktivist 3. Organized crime 4. Nation states/APT 5. Insiders 6. Competitors 2. Attributes of actors 1. Internal/external 2. Level of sophistication 3. Resources/funding 4. Intent/motivation 3. Use of open-source intelligence
Explain penetration testing concepts.	1. Active reconnaissance 2. Passive reconnaissance 3. Pivot 4. Initial exploitation 5. Persistence 6. Escalation of privilege 7. Black box 8. White box 9. Gray box 10. Penetration testing vs. vulnerability scanning
Explain vulnerability scanning concepts.	1.Passively test security controls 2. Identify vulnerability 3. Identify lack of security controls 4. Identify common misconfigurations 5. Intrusive vs. non-intrusive 6. Credentialed vs. non-credentialed 7. False positive
Explain the impact associated with types of vulnerabilities.	1. Race conditions 2. Vulnerabilities due to: 1. End-of-life systems 2. Embedded systems 3. Lack of vendor support 3. Improper input handling 4. Improper error handling 5. Misconfiguration/weak configuration 6. Default configuration 7. Resource exhaustion 8. Untrained users 9. Improperly configured accounts 10. Vulnerable business processes

Topic	Details
	11. Weak cipher suites and implementations 12. Memory/buffer vulnerability 1. Memory leak 2. Integer overflow 3. Buffer overflow 4. Pointer dereference 5. DLL injection 13. System sprawl/undocumented assets 14. Architecture/design weaknesses 15. New threats/zero day 16. Improper certificate and key management
Technologies and Tools 22%	
Install and configure network components, both hardwareand software-based, to support organizational security.	1. Firewall 1. ACL 2. Application-based vs. network-based 3. Stateful vs. stateless 4. Implicit deny 2. VPN concentrator 1. Remote access vs. site-to-site 2. IPSec 3. Tunnel mode 4. Transport mode 5. AH 6. ESP 7. Split tunnel vs. full tunnel 8. TLS 9. Always-on VPN 3. NIPS/NIDS 1. Signature-based 2. Heuristic/behavioral 3. Anomaly 4. Inline vs. passive 5. In-band vs. out-of-band 6. Rules 7. Analytics 8. False positive 9. False negative 4. Router

Topic	Details
	1. ACLs 2. Antispoofing 5. Switch 1. Port security 2. Layer 2 vs. Layer 3 3. Loop prevention 4. Flood guard 6. Proxy 1. Forward and reverse proxy 2. Transparent 3. Application/multipurpose 7. Load balancer 1. Scheduling 2. Affinity 3. Round-robin 4. Active-passive 5. Active-active 6. Virtual IPs 8. Access point 1. SSID 2. MAC filtering 3. Signal strength 4. Band selection/width 5. Antenna types and placement 6. Fat vs. thin 7. Controller-based vs. standalone 9. SIEM 1. Aggregation 2. Correlation 3. Automated alerting and triggers 4. Time synchronization 5. Event deduplication 6. Logs/WORM 10. DLP 1. USB blocking

Topic	Details
	2. Cloud-based 3. Email 11. NAC 1. Dissolvable vs. permanent 2. Host health checks 3. Agent vs. agentless 12. Mail gateway 1. Spam filter 2. DLP 3. Encryption 13. Bridge 14. SSL/TLS accelerators 15. SSL decryptors 16. Media gateway 17. Hardware security module
Given a scenario, use appropriate software tools to assess the security posture of an organization.	1. Protocol analyzer 2. Network scanners 1. Rogue system detection 2. Network mapping 3. Wireless scanners/cracker 4. Password cracker 5. Vulnerability scanner 6. Configuration compliance scanner 7. Exploitation frameworks 8. Data sanitization tools 9. Steganography tools 10. Honeypot 11. Backup utilities 12. Banner grabbing 13. Passive vs. active 14. Command line tools 1. ping 2. netstat 3. tracert 4. nslookup/dig 5. arp 6. ipconfig/ip/ifconfig 7. tcpdump 8. nmap

Topic	Details
	9. netcat
Given a scenario, troubleshoot common security issues.	1. Unencrypted credentials/clear text 2. Logs and events anomalies 3. Permission issues 4. Access violations 5. Certificate issues 6. Data exfiltration 7. Misconfigured devices 1. Firewall 2. Content filter 3. Access points 8. Weak security configurations 9. Personnel issues 1. Policy violation 2. Insider threat 3. Social engineering 4. Social media 5. Personal email 10. Unauthorized software 11. Baseline deviation 12. License compliance violation (availability/integrity) 13. Asset management 14. Authentication issues
Given a scenario, analyze and interpret output from security technologies.	1. HIDS/HIPS 2. Antivirus 3. File integrity check 4. Host-based firewall 5. Application whitelisting 6. Removable media control 7. Advanced malware tools 8. Patch management tools 9. UTM 10. DLP 11. Data execution prevention 12. Web application firewall
Given a scenario, deploy mobile devices securely.	1. Connection methods 1. Cellular 2. WiFi 3. SATCOM 4. Bluetooth 5. NFC

Topic	Details
	6. ANT 7. Infrared 8. USB 2. Mobile device management concepts 1. Application management 2. Content management 3. Remote wipe 4. Geofencing 5. Geolocation 6. Screen locks 7. Push notification services 8. Passwords and pins 9. Biometrics 10. Context-aware authentication 11. Containerization 12. Storage segmentation 13. Full device encryption 3. Enforcement and monitoring for: 1. Third-party app stores 2. Rooting/jailbreaking 3. Sideloading 4. Custom firmware 5. Carrier unlocking 6. Firmware OTA updates 7. Camera use 8. SMS/MMS 9. External media 10. USB OTG 11. Recording microphone 12. GPS tagging 13. WiFi direct/ad hoc 14. Tethering 15. Payment methods 4. Deployment models 1. BYOD 2. COPE 3. CYOD 4. Corporate-owned 5. VDI

Topic	Details
Given a scenario, implement secure protocols.	1. Protocols 1. DNSSEC 2. SSH 3. S/MIME 4. SRTP 5. LDAPS 6. FTPS 7. SFTP 8. SNMPv3 9. SSL/TLS 10. HTTPS 11. Secure POP/IMAP 2. Use cases 1. Voice and video 2. Time synchronization 3. Email and web 4. File transfer 5. Directory services 6. Remote access 7. Domain name resolution 8. Routing and switching 9. Network address allocation 10. Subscription services
Architecture and Design 15%	
Explain use cases and purpose for frameworks, best practices and secure configuration guides.	1. Industry-standard frameworks and reference architectures 1. Regulatory 2. Non-regulatory 3. National vs. international 4. Industry-specific frameworks 2. Benchmarks/secure configuration guides 1. Platform/vendor-specific guides 2. Web server 3. Operating system 4. Application server 5. Network infrastructure devices 6. General purpose guides 3. Defense-in-depth/layered security

Topic	Details
	1. Vendor diversity 2. Control diversity 3. Administrative 4. Technical 5. User training
Given a scenario, implement secure network architecture concepts.	1. Zones/topologies 1. DMZ 2. Extranet 3. Intranet 4. Wireless 5. Guest 6. Honeynets 7. NAT 8. Ad hoc 2. Segregation/segmentation/isolation 1. Physical 2. Logical (VLAN) 3. Virtualization 4. Air gaps 3. Tunneling/VPN 1. Site-to-site 2. Remote access 4. Security device/technology placement 1. Sensors 2. Collectors 3. Correlation engines 4. Filters 5. Proxies 6. Firewalls 7. VPN concentrators 8. SSL accelerators 9. Load balancers 10. DDoS mitigator 11. Aggregation switches 12. Taps and port mirror 5. SDN

Topic	Details
Given a scenario, implement secure systems design.	1. Hardware/firmware security 1. FDE/SED 2. TPM 3. HSM 4. UEFI/BIOS 5. Secure boot and attestation 6. Supply chain 7. Hardware root of trust 8. EMI/EMP 2. Operating systems 1. Types 2. Network 3. Server 4. Workstation 5. Appliance 6. Kiosk 7. Mobile OS 8. Patch management 9. Disabling unnecessary ports and services 10. Least functionality 11. Secure configurations 12. Trusted operating system 13. Application whitelisting/blacklisting 14. Disable default accounts/passwords 3. Peripherals 1. Wireless keyboards 2. Wireless mice 3. Displays 4. WiFi-enabled MicroSD cards 5. Printers/MFDs 6. External storage devices 7. Digital cameras
Explain the importance of secure staging deployment concepts.	1. Sandboxing 2. Environment 1. Development 2. Test 3. Staging 4. Production

Topic	Details
	3. Secure baseline Integrity measurement
Explain the security implications of embedded systems.	1. SCADA/ICS 2. Smart devices/IoT 1. Wearable technology 2. Home automation 3. HVAC 4. SoC 5. RTOS 6. Printers/MFDs 7. Camera systems 8. Special purpose 1. Medical devices 2. Vehicles 3. Aircraft/UAV
Summarize secure application development and deployment concepts.	1. Development life-cycle models 1. Waterfall vs. Agile 2. Secure DevOps 1. Security automation 2. Continuous integration 3. Baselining 4. Immutable systems 5. Infrastructure as code 3. Version control and change management 4. Provisioning and deprovisioning 5. Secure coding techniques 1. Proper error handling 2. Proper input validation 3. Normalization 4. Stored procedures 5. Code signing 6. Encryption 7. Obfuscation/camouflage 8. Code reuse/dead code 9. Server-side vs. client-side execution and validation 10. Memory management 11. Use of third-party libraries and SDKs

Topic	Details
	12. Data exposure 6. Code quality and testing 1. Static code analyzers 2. Dynamic analysis (e.g., fuzzing) 3. Stress testing 4. Sandboxing 5. Model verification 7. Compiled vs. runtime code
Summarize cloud and virtualization concepts.	1. Hypervisor 1. Type I 2. Type II 3. Application cells/containers 2. VM sprawl avoidance 3. VM escape protection 4. Cloud storage 5. Cloud deployment models 1. SaaS 2. PaaS 3. IaaS 4. Private 5. Public 6. Hybrid 7. Community 6. On-premise vs. hosted vs. cloud 7. VDI/VDE 8. Cloud access security broker 9. Security as a Service
Explain how resiliency and automation strategies reduce risk.	1. Automation/scripting 1. Automated courses of action 2. Continuous monitoring 3. Configuration validation 2. Templates 3. Master image 4. Non-persistence 1. Snapshots 2. Revert to known state

Topic	**Details**
	3. Rollback to known configuration 4. Live boot media 5. Elasticity 6. Scalability 7. Distributive allocation 8. Redundancy 9. Fault tolerance 10. High availability 11. RAID
Explain the importance of physical security controls.	1. Lighting 2. Signs 3. Fencing/gate/cage 4. Security guards 5. Alarms 6. Safe 7. Secure cabinets/enclosures 8. Protected distribution/Protected cabling 9. Airgap 10. Mantrap 11. Faraday cage 12. Lock types 13. Biometrics 14. Barricades/bollards 15. Tokens/cards 16. Environmental controls 1. HVAC 2. Hot and cold aisles 3. Fire suppression 17. Cable locks 18. Screen filters 19. Cameras 20. Motion detection 21. Logs 22. Infrared detection 23. Key management
Identity and Access Management 16%	
Compare and contrast identity and access management concepts	1. Identification, authentication, authorization and accounting (AAA) 2. Multifactor authentication 1. Something you are 2. Something you have 3. Something you know

Topic	Details
	4. Somewhere you are 5. Something you do 3. Federation 4. Single sign-on 5. Transitive trust
Given a scenario, install and configure identity and access services.	1. LDAP 2. Kerberos 3. TACACS+ 4. CHAP 5. PAP 6. MSCHAP 7. RADIUS 8. SAML 9. OpenID Connect 10. OAUTH 11. Shibboleth 12. Secure token 13. NTLM
Given a scenario, implement identity and access management controls.	1. Access control models 1. MAC 2. DAC 3. ABAC 4. Role-based access control 5. Rule-based access control 2. Physical access control 1. Proximity cards 2. Smart cards 3. Biometric factors 1. Fingerprint scanner 2. Retinal scanner 3. Iris scanner 4. Voice recognition 5. Facial recognition 6. False acceptance rate 7. False rejection rate 8. Crossover error rate 4. Tokens 1. Hardware 2. Software

Topic	Details
	3. HOTP/TOTP 5. Certificate-based authentication 1. PIV/CAC/smart card 2. IEEE 802.1x 6. File system security 7. Database security
Given a scenario, differentiate common account management practices.	1. Account types 1. User account 2. Shared and generic accounts/credentials 3. Guest accounts 4. Service accounts 5. Privileged accounts 2. General Concepts 1. Least privilege 2. Onboarding/offboarding 3. Permission auditing and review 4. Usage auditing and review 5. Time-of-day restrictions 6. Recertification 7. Standard naming convention 8. Account maintenance 9. Group-based access control 10. Location-based policies 3. Account policy enforcement 1. Credential management 2. Group policy 3. Password complexity 4. Expiration 5. Recovery 6. Disablement 7. Lockout 8. Password history 9. Password reuse 10. Password length
Risk Management 14%	
Explain the importance of policies, plans and	1. Standard operating procedure 2. Agreement types

Topic	Details
procedures related to organizational security	1. BPA 2. SLA 3. ISA 4. MOU/MOA 3. Personnel management 1. Mandatory vacations 2. Job rotation 3. Separation of duties 4. Clean desk 5. Background checks 6. Exit interviews 7. Role-based awareness training 8. Data owner 9. System administrator 10. System owner 11. User 12. Privileged user 13. Executive user 14. NDA 15. Onboarding 16. Continuing education 17. Acceptable use policy/rules of behavior 18. Adverse actions 4. General security policies 1. Social media networks/applications 2. Personal email
Summarize business impact analysis concepts.	1. RTO/RPO 2. MTBF 3. MTTR 4. Mission-essential functions 5. Identification of critical systems 6. Single point of failure 7. Impact 1. Life 2. Property 3. Safety 4. Finance 5. Reputation

Topic	Details
	8. Privacy impact assessment 9. Privacy threshold assessment
Explain risk management processes and concepts.	1. Threat assessment 1. Environmental 2. Manmade 3. Internal vs. external 2. Risk assessment 1. SLE 2. ALE 3. ARO 4. Asset value 5. Risk register 6. Likelihood of occurrence 7. Supply chain assessment 8. Impact 9. Quantitative 10. Qualitative 11. Testing 12. Penetration testing authorization 13. Vulnerability testing authorization 14. Risk response techniques 15. Accept 16. Transfer 17. Avoid 18. Mitigate 3. Change management
Given a scenario, follow incident response procedures.	1. Incident response plan 1. Documented incident types/category definitions 2. Roles and responsibilities 3. Reporting requirements/escalation 4. Cyber-incident response teams 5. Exercise 2. Incident response process 1. Preparation 2. Identification 3. Containment 4. Eradication 5. Recovery

Topic	Details
	6. Lessons learned
Summarize basic concepts of forensics.	1. Order of volatility 2. Chain of custody 3. Legal hold 4. Data acquisition 1. Capture system image 2. Network traffic and logs 3. Capture video 4. Record time offset 5. Take hashes 6. Screenshots 7. Witness interviews 5. Preservation 6. Recovery 7. Strategic intelligence/ counterintelligence gathering 1. Active logging 8. Track man-hours
Explain disaster recovery and continuity of operation concepts.	1. Recovery sites 1. Hot site 2. Warm site 3. Cold site 2. Order of restoration 3. Backup concepts 1. Differential 2. Incremental 3. Snapshots 4. Full 4. Geographic considerations 1. Off-site backups 2. Distance 3. Location selection 4. Legal implications 5. Data sovereignty 5. Continuity of operation planning

Topic	Details
	1. Exercises/tabletop 2. After-action reports 3. Failover 4. Alternate processing sites 5. Alternate business practices
Compare and contrast various types of controls.	1. Deterrent 2. Preventive 3. Detective 4. Corrective 5. Compensating 6. Technical 7. Administrative 8. Physical
Given a scenario, carry out data security and privacy practices.	1. Data destruction and media sanitization 1. Burning 2. Shredding 3. Pulping 4. Pulverizing 5. Degaussing 6. Purging 7. Wiping 2. Data sensitivity labeling and handling 1. Confidential 2. Private 3. Public 4. Proprietary 5. PII 6. PHI 3. Data roles 1. Owner 2. Steward/custodian 3. Privacy officer 4. Data retention 5. Legal and compliance
Cryptography and PKI 12%	
Compare and contrast basic concepts of cryptography.	1. Symmetric algorithms 2. Modes of operation 3. Asymmetric algorithms 4. Hashing

Topic	Details
	5. Salt, IV, nonce 6. Elliptic curve 7. Weak/deprecated algorithms 8. Key exchange 9. Digital signatures 10. Diffusion 11. Confusion 12. Collision 13. Steganography 14. Obfuscation 15. Stream vs. block 16. Key strength 17. Session keys 18. Ephemeral key 19. Secret algorithm 20. Data-in-transit 21. Data-at-rest 22. Data-in-use 23. Random/pseudo-random number generation 24. Key stretching 25. Implementation vs. algorithm selection 1. Crypto service provider 2. Crypto modules 26. Perfect forward secrecy 27. Security through obscurity 28. Common use cases 1. Low power devices 2. Low latency 3. High resiliency 4. Supporting confidentiality 5. Supporting integrity 6. Supporting obfuscation 7. Supporting authentication 8. Supporting non-repudiation 9. Resource vs. security constraints
Explain cryptography algorithms and their basic characteristics.	1. Symmetric algorithms 1. AES 2. DES 3. 3DES 4. RC4 5. Blowfish/Twofish

Topic	Details
	2. Cipher modes 1. CBC 2. GCM 3. ECB 4. CTR 5. Stream vs. block 3. Asymmetric algorithms 1. RSA 2. DSA 3. Diffie-Hellman 4. Groups 5. DHE 6. ECDHE 7. Elliptic curve 8. PGP/GPG 4. Hashing algorithms 1. MD5 2. SHA 3. HMAC 4. RIPEMD 5. Key stretching algorithms 1. BCRYPT 2. PBKDF2 6. Obfuscation 1. XOR 2. ROT13 3. Substitution ciphers
Given a scenario, install and configure wireless security settings.	1. Cryptographic protocols 1. WPA 2. WPA2 3. CCMP 4. TKIP 2. Authentication protocols 1. EAP

Topic	Details
	2. PEAP 3. EAP-FAST 4. EAP-TLS 5. EAP-TTLS 6. IEEE 802.1x 7. RADIUS Federation 3. Methods 1. PSK vs. Enterprise vs. Open 2. WPS 3. Captive portals
Given a scenario, implement public key infrastructure.	1. Components 1. CA 2. Intermediate CA 3. CRL 4. OCSP 5. CSR 6. Certificate 7. Public key 8. Private key 9. Object identifiers (OID) 2. Concepts 1. Online vs. offline CA 2. Stapling 3. Pinning 4. Trust model 5. Key escrow 6. Certificate chaining 3. Types of certificates 1. Wildcard 2. SAN 3. Code signing 4. Self-signed 5. Machine/computer 6. Email 7. User 8. Root 9. Domain validation 10. Extended validation

Topic	Details
	4. Certificate formats 1. DER 2. PEM 3. PFX 4. CER 5. P12 6. P7B

SY0-501 Sample Questions:

01. Which of the following reduces the effectiveness of a good password policy?
a) Account lockout
b) Password recovery
c) Account disablement
d) Password reuse

02. You identify a system that becomes progressively slower over a couple days until it is unresponsive. Which of the following is most likely the reason for this behavior?
a) Improper error handling
b) Race condition
c) Memory leak
d) Untrained user

03. Which one of the following best provides an example of detective controls versus prevention controls?
a) IDS/camera versus IPS/guard
b) IDS/IPS versus camera/guard
c) IPS/camera versus IDS/guard
d) IPS versus guard

04. An organization is implementing a server-side application using OAuth 2.0. Which of the following grant types should be used?
a) Implicit
b) Authorization code
c) Password credentials
d) Client credentials

05. Which of the following is associated with certificate issues?
a) Unauthorized transfer of data
b) Release of private or confidential information
c) Algorithm mismatch error
d) Prevention of legitimate content

06. Eliminating email to avoid the risk of email-borne viruses is an effective solution but is not likely to be a realistic approach for which of the following?
a) Risk avoidance
b) Risk transference
c) Risk acceptance
d) Risk mitigation

07. Which of the following best describes a biometric false acceptance rate (FAR)?
a) The point at which acceptances and rejections are equal
b) Rejection of an authorized user
c) Access allowed to an unauthorized user
d) Failure to identify a biometric image

08. Advanced malware tools use which of the following analysis methods?
a) Static analysis
b) Context based
c) Signature analysis
d) Manual analysis

09. If the organization requires a firewall feature that controls network activity associated with DoS attacks, which of the following safeguards should be implemented?
a) Loop protection
b) Flood guard
c) Implicit deny
d) Port security

10. Which of the following is not a certificate trust model for arranging Certificate Authorities?
a) Bridge CA architecture
b) Hierarchical CA architecture
c) Single-CA architecture
d) Sub-CA architecture

Answers to SY0-501 Exam Questions:

Question: 01 Answer: d	Question: 02 Answer: c	Question: 03 Answer: a	Question: 04 Answer: b	Question: 05 Answer: c
Question: 06 Answer: a	Question: 07 Answer: c	Question: 08 Answer: b	Question: 09 Answer: b	Question: 10 Answer: d

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@edusum.com