EDUSUM
#1 Online Certification Guide

COMPTIA SY0-501

CompTIA Security+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

SY0-501
CompTIA Security+
90 Questions Exam – 750/900 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your SY0-501 Certification Well:

The SY0-501 is best suitable for candidates who want to gain knowledge in the CompTIA Core. Before you start your SY0-501 preparation you may struggle to get all the crucial Security+ materials like SY0-501 syllabus, sample questions, study guide.

But don't worry the SY0-501 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the SY0-501 syllabus?
- How many questions are there in the SY0-501 exam?
- Which Practice test would help me to pass the SY0-501 exam at the first attempt?

Passing the SY0-501 exam makes you CompTIA Security+. Having the Security+ certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CompTIA SY0-501 Security+ Certification Details:

Exam Name	CompTIA Security+
Exam Code	SY0-501
Exam Price	$370 (USD)
Duration	90 mins
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**

SY0-501 Syllabus:

Topic	Details
Threats, Attacks and Vulnerabilities - 21%	
Given a scenario, analyze indicators of compromise and determine the type of malware.	- Viruses - Crypto-malware - Ransomware - Worm - Trojan - Rootkit - Keylogger - Adware - Spyware - Bots - RAT - Logic bomb - Backdoor
Compare and contrast types of attacks.	1. Social engineering • Phishing • Spear phishing • Whaling • Vishing • Tailgating • Impersonation • Dumpster diving • Shoulder surfing • Hoax • Watering hole attack • Principles (reasons for effectiveness) 1. Authority 2. Intimidation 3. Consensus 4. Scarcity 5. Familiarity 6. Trust 7. Urgency 2. Application/service attacks

Topic	Details
	• DoS • DDoS • Man-in-the-middle • Buffer overflow • Injection • Cross-site scripting • Cross-site request forgery • Privilege escalation • ARP poisoning • Amplification • DNS poisoning • Domain hijacking • Man-in-the-browser • Zero day • Replay • Pass the hash • Hijacking and related attacks 1. Clickjacking 2. Session hijacking 3. URL hijacking 4. Typo squatting • Driver manipulation 1. Shimming 2. Refactoring • MAC spoofing • 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

Topic	Details
	11. Disassociation 4. Cryptographic attacks • Birthday • Known plain text/cipher text • Rainbow tables • Dictionary • Brute force 1. Online vs. offline • Collision • Downgrade • Replay • Weak implementations
Explain threat actor types and attributes.	1. Types of actors • Script kiddies • Hacktivist • Organized crime • Nation states/APT • Insiders • Competitors 2. Attributes of actors • Internal/external • Level of sophistication • Resources/funding • Intent/motivation 3. Use of open-source intelligence
Explain penetration testing concepts.	- Active reconnaissance - Passive reconnaissance - Pivot - Initial exploitation - Persistence - Escalation of privilege - Black box - White box

Topic	Details
	- Gray box - Penetration testing vs. vulnerability scanning
Explain vulnerability scanning concepts.	- Passively test security controls - Identify vulnerability - Identify lack of security controls - Identify common misconfigurations - Intrusive vs. non-intrusive - Credentialed vs. non-credentialed - False positive
Explain the impact associated with types of vulnerabilities.	1. Race conditions 2. Vulnerabilities due to: • End-of-life systems • Embedded systems • 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 11. Weak cipher suites and implementations 12. Memory/buffer vulnerability • Memory leak • Integer overflow • Buffer overflow • Pointer dereference • 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,	1. Firewall • ACL • Application-based vs. network-based

Topic	Details
to support organizational security.	• Stateful vs. stateless • Implicit deny 2. VPN concentrator • Remote access vs. site-to-site • IPSec 1. Tunnel mode 2. Transport mode 3. AH 4. ESP • Split tunnel vs. full tunnel • TLS • Always-on VPN 3. NIPS/NIDS • Signature-based • Heuristic/behavioral • Anomaly • Inline vs. passive • In-band vs. out-of-band • Rules • Analytics 1. False positive 2. False negative 4. Router • ACLs • Antispoofing 5. Switch • Port security • Layer 2 vs. Layer 3 • Loop prevention • Flood guard 6. Proxy • Forward and reverse proxy

Topic	Details
	• Transparent • Application/multipurpose 7. Load balancer • Scheduling 1. Affinity 2. Round-robin • Active-passive • Active-active • Virtual IPs 8. Access point • SSID • MAC filtering • Signal strength • Band selection/width • Antenna types and placement • Fat vs. thin • Controller-based vs. standalone 9. SIEM • Aggregation • Correlation • Automated alerting and triggers • Time synchronization • Event deduplication • Logs/WORM 10. DLP • USB blocking • Cloud-based • Email 11. NAC • Dissolvable vs. permanent • Host health checks • Agent vs. agentless

Topic	Details
	12. Mail gateway • Spam filter • DLP • 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 • Rogue system detection • 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 • ping • netstat • tracert • nslookup/dig • arp • ipconfig/ip/ifconfig • tcpdump • nmap • netcat
Given a scenario, troubleshoot common security issues.	1. Unencrypted credentials/clear text 2. Logs and events anomalies 3. Permission issues 4. Access violations

Topic	Details
	5. Certificate issues 6. Data exfiltration 7. Misconfigured devices • Firewall • Content filter • Access points 8. Weak security configurations 9. Personnel issues • Policy violation • Insider threat • Social engineering • Social media • 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 • Cellular • WiFi • SATCOM • Bluetooth • NFC • ANT

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

Topic	Details
	• COPE • CYOD • Corporate-owned • VDI
Given a scenario, implement secure protocols.	1. Protocols • DNSSEC • SSH • S/MIME • SRTP • LDAPS • FTPS • SFTP • SNMPv3 • SSL/TLS • HTTPS • Secure POP/IMAP 2. 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
Architecture and Design - 15%	
Explain use cases and purpose for frameworks, best practices and secure configuration guides.	1. Industry-standard frameworks and reference architectures • Regulatory • Non-regulatory • National vs. international • Industry-specific frameworks

Topic	Details
	2. Benchmarks/secure configuration guides • Platform/vendor-specific guides • Web server • Operating system • Application server • Network infrastructure devices • General purpose guides 3. Defense-in-depth/layered security • Vendor diversity • Control diversity • Administrative • Technical • User training
Given a scenario, implement secure network architecture concepts.	1. Zones/topologies • DMZ • Extranet • Intranet • Wireless • Guest • Honeynets • NAT • Ad hoc 2. Segregation/segmentation/isolation • Physical • Logical (VLAN) • Virtualization • Air gaps 3. Tunneling/VPN • Site-to-site • Remote access 4. Security device/technology placement • Sensors

Topic	Details
	• Collectors • Correlation engines • Filters • Proxies • Firewalls • VPN concentrators • SSL accelerators • Load balancers • DDoS mitigator • Aggregation switches • Taps and port mirror 5. SDN
Given a scenario, implement secure systems design.	1. Hardware/firmware security • FDE/SED • TPM • HSM • UEFI/BIOS • Secure boot and attestation • Supply chain • Hardware root of trust • EMI/EMP 2. Operating systems • Types 1. Network 2. Server 3. Workstation 4. Appliance 5. Kiosk 6. Mobile OS • Patch management • Disabling unnecessary ports and services • Least functionality • Secure configurations • Trusted operating system • Application whitelisting/blacklisting

Topic	Details
	- Disable default accounts/passwords 3. Peripherals - Wireless keyboards - Wireless mice - Displays - WiFi-enabled MicroSD cards - Printers/MFDs - External storage devices - Digital cameras
Explain the importance of secure staging deployment concepts.	1. Sandboxing 2. Environment - Development - Test - Staging - Production 3. Secure baseline 4. Integrity measurement
Explain the security implications of embedded systems.	1. SCADA/ICS 2. Smart devices/IoT - Wearable technology - Home automation 3. HVAC 4. SoC 5. RTOS 6. Printers/MFDs 7. Camera systems 8. Special purpose - Medical devices - Vehicles - Aircraft/UAV
Summarize secure application development and deployment concepts.	1. Development life-cycle models - Waterfall vs. Agile 2. Secure DevOps

Topic	Details
	• Security automation • Continuous integration • Baselining • Immutable systems • Infrastructure as code 3. Version control and change management 4. Provisioning and deprovisioning 5. Secure coding techniques • Proper error handling • Proper input validation • Normalization • Stored procedures • Code signing • Encryption • Obfuscation/camouflage • Code reuse/dead code • Server-side vs. client-side execution and validation • Memory management • Use of third-party libraries and SDKs • Data exposure 6. Code quality and testing • Static code analyzers • Dynamic analysis (e.g., fuzzing) • Stress testing • Sandboxing • Model verification 7. Compiled vs. runtime code
Summarize cloud and virtualization concepts.	1. Hypervisor • Type I • Type II • Application cells/containers 2. VM sprawl avoidance 3. VM escape protection

Topic	Details
	4. Cloud storage 5. Cloud deployment models • SaaS • PaaS • IaaS • Private • Public • Hybrid • 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 • Automated courses of action • Continuous monitoring • Configuration validation 2. Templates 3. Master image 4. Non-persistence • Snapshots • Revert to known state • Rollback to known configuration • 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

Topic	Details
	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 • HVAC • Hot and cold aisles • 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 • Something you are • Something you have • Something you know • Somewhere you are • Something you do 3. Federation 4. Single sign-on 5. Transitive trust
Given a scenario, install and configure identity and access services.	- LDAP - Kerberos - TACACS+ - CHAP - PAP

Topic	Details
	- MSCHAP - RADIUS - SAML - OpenID Connect - OAUTH - Shibboleth - Secure token - NTLM
Given a scenario, implement identity and access management controls.	1. Access control models • MAC • DAC • ABAC • Role-based access control • Rule-based access control 2. Physical access control • Proximity cards • Smart cards 3. Biometric factors • Fingerprint scanner • Retinal scanner • Iris scanner • Voice recognition • Facial recognition • False acceptance rate • False rejection rate • Crossover error rate 4. Tokens • Hardware • Software • HOTP/TOTP 5. Certificate-based authentication • PIV/CAC/smart card • IEEE 802.1x

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

Topic	Details
related to organizational security	- BPA - SLA - ISA - MOU/MOA 3. Personnel management - Mandatory vacations - Job rotation - Separation of duties - Clean desk - Background checks - Exit interviews - Role-based awareness training 1. Data owner 2. System administrator 3. System owner 4. User 5. Privileged user 6. Executive user 7. NDA 8. Onboarding 9. Continuing education 10. Acceptable use policy/rules of behavior 11. Adverse actions 4. General security policies - Social media networks/applications - 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 - Life - Property

Topic	Details
	- Safety - Finance - Reputation 8. Privacy impact assessment 9. Privacy threshold assessment
Explain risk management processes and concepts.	1. Threat assessment - Environmental - Manmade - Internal vs. external 2. Risk assessment - SLE - ALE - ARO - Asset value - Risk register - Likelihood of occurrence - Supply chain assessment - Impact - Quantitative - Qualitative - Testing 1. Penetration testing authorization 2. Vulnerability testing 3. authorization - Risk response techniques 1. Accept 2. Transfer 3. Avoid 4. Mitigate 3. Change management
Given a scenario, follow incident response procedures.	1. Incident response plan - Documented incident types/category definitions

Topic	Details
	- Roles and responsibilities - Reporting requirements/escalation - Cyber-incident response teams - Exercise 2. Incident response process - Preparation - Identification - Containment - Eradication - Recovery - Lessons learned
Summarize basic concepts of forensics.	1. Order of volatility 2. Chain of custody 3. Legal hold 4. Data acquisition - Capture system image - Network traffic and logs - Capture video - Record time offset - Take hashes - Screenshots - Witness interviews 5. Preservation 6. Recovery 7. Strategic intelligence/ counterintelligence gathering - Active logging 8. Track man-hours
Explain disaster recovery and continuity of operation concepts.	1. Recovery sites - Hot site - Warm site - Cold site 2. Order of restoration 3. Backup concepts

Topic	Details
	• Differential • Incremental • Snapshots • Full 4. Geographic considerations • Off-site backups • Distance • Location selection • Legal implications • Data sovereignty 5. Continuity of operation planning • Exercises/tabletop • After-action reports • Failover • Alternate processing sites • Alternate business practices
Compare and contrast various types of controls.	- Deterrent - Preventive - Detective - Corrective - Compensating - Technical - Administrative - Physical
Given a scenario, carry out data security and privacy practices.	1. Data destruction and media sanitization • Burning • Shredding • Pulping • Pulverizing • Degaussing • Purging • Wiping 2. Data sensitivity labeling and handling • Confidential

Topic	Details
	- Private - Public - Proprietary - PII - PHI 3. Data roles - Owner - Steward/custodian - 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 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

Topic	Details
	• Crypto service provider • Crypto modules 26. Perfect forward secrecy 27. Security through obscurity 28. 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
Explain cryptography algorithms and their basic characteristics.	1. Symmetric algorithms • AES • DES • 3DES • RC4 • Blowfish/Twofish 2. Cipher modes • CBC • GCM • ECB • CTR • Stream vs. block 3. Asymmetric algorithms • RSA • DSA • Diffie-Hellman 1. Groups 2. DHE 3. ECDHE

Topic	Details
	• Elliptic curve • PGP/GPG 4. Hashing algorithms • MD5 • SHA • HMAC • RIPEMD 5. Key stretching algorithms • BCRYPT • PBKDF2 6. Obfuscation • XOR • ROT13 • Substitution ciphers
Given a scenario, install and configure wireless security settings.	1. Cryptographic protocols • WPA • WPA2 • CCMP • TKIP 2. Authentication protocols • EAP • PEAP • EAP-FAST • EAP-TLS • EAP-TTLS • IEEE 802.1x • RADIUS Federation 3. Methods • PSK vs. Enterprise vs. Open • WPS • Captive portals

Topic	Details
Given a scenario, implement public key infrastructure.	1. Components • CA • Intermediate CA • CRL • OCSP • CSR • Certificate • Public key • Private key • Object identifiers (OID) 2. Concepts • Online vs. offline CA • Stapling • Pinning • Trust model • Key escrow • Certificate chaining 3. Types of certificates • Wildcard • SAN • Code signing • Self-signed • Machine/computer • Email • User • Root • Domain validation • Extended validation 4. Certificate formats • DER • PEM • PFX • CER • P12 • P7B

CompTIA SY0-501 Sample Questions:

Question: 1

Which of the following if used would BEST reduce the number of successful phishing attacks?

a) Two-factor authentication
b) Application layer firewall
c) Mantraps
d) User training

Answer: d

Question: 2

A security administrator discovers that an attacker used a compromised host as a platform for launching attacks deeper into a company's network.

What terminology BEST describes the use of the compromised host?

a) Brute force
b) Active reconnaissance
c) Pivoting
d) Passing point

Answer: c

Question: 3

A system administrator is configuring accounts on a newly established server. Which of the following characteristics BEST differentiates service accounts from other types of accounts?

a) They can often be restricted in privilege.
b) They are meant for non-person entities.
c) They require special permissions to OS files and folders.
d) They remain disabled in operations.
e) They do not allow passwords to be set.

Answer: b

Question: 4

Company A has just developed a bespoke system for booking airline tickets. What is it called if a freelance coding specialist tests it for security flaws?

a) Code review
b) Static code review
c) Regression testing
d) Dynamic code review

Answer: c

Question: 5

Which of the following is a measure of reliability?

a) MTTR
b) MTBF
c) MTTF
d) RPO

Answer: b

Question: 6

A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following will you choose?

a) L2TP/IPSec
b) SSL VPN
c) PPTP VPN
d) IKEv2 VPN

Answer: b

Question: 7

Joe, a security analyst, is asked by a co-worker, "What is this AAA thing all about in the security world? Sounds like something I can use for my car."

Which of the following terms should Joe discuss in his response to his co-worker?

(Select THREE).

a) Accounting
b) Accountability
c) Authorization
d) Authentication
e) Access
f) Agreement

Answer: a, c, d

Question: 8

Recently, a company has been facing an issue with shoulder surfing. Which of the following safeguards would help with this?

a) Screen filters
b) Biometric authentication
c) Smart cards
d) Video cameras

Answer: a

Question: 9

An input field that is accepting more data than has been allocated for it in memory is an attribute of:

a) buffer overflow.
b) memory leak.
c) cross-site request forgery.
d) resource exhaustion.

Answer: a

Question: 10

The process of presenting a user ID to a validating system is known as:

a) authorization.
b) authentication.
c) identification.
d) single sign-on.

Answer: c

Study Guide to Crack CompTIA Security+ SY0-501 Exam:

- Getting details of the SY0-501 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the SY0-501 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CompTIA provided training for SY0-501 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the SY0-501 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on SY0-501 practice tests is must. Continuous practice will make you an expert in all syllabus areas.