## **CompTIA Security+ (SY0-701) Practice Test 1 – All Answers & Explanations**

### **1. A) Encrypting sensitive files before transmission**

Encryption ensures that only authorized recipients can access data, fulfilling the principle of confidentiality.

### **2. B) ISO 27001**

ISO 27001 provides a framework for establishing and improving an information security management system.

### **3. C) Resources are accessible when needed**

Availability ensures that users can access resources when required, minimizing downtime.

### **4. D) Mandatory Access Control (MAC)**

MAC enforces strict access policies defined by administrators, not users.

### **5. A) Users have minimal access necessary to perform their tasks**

Least privilege reduces risk by giving users only the permissions they need.

### **6. C) Trojan**

Trojans disguise themselves as legitimate software to trick users into installing malicious programs.

### **7. A) Pharming**

Pharming alters DNS entries to redirect users to malicious websites.

### **8. C) An attacker posing as IT support to obtain user credentials**

This is a classic example of social engineering—manipulating people, not systems.

### **9. D) Zero-day exploit**

Zero-days are vulnerabilities unknown to vendors and exploited before patches exist.

### **10. A) Detect and log unauthorized access attempts**

Honeypots are traps that help security teams monitor and analyze attacker behavior.

### **11. B) A subnet that hosts public-facing services and isolates them from the internal network**

DMZs provide controlled access to services like web or email servers while protecting internal assets.

### **12. A) Isolates workloads to reduce the attack surface**

Micro-segmentation helps limit lateral movement in case of a breach.

### **13. C) Intrusion Prevention System (IPS)**

IPS actively blocks suspicious traffic based on signatures or behavior.

### **14. B) Encrypt communications over insecure networks**

VPNs protect data confidentiality by creating secure tunnels.

### **15. B) Private cloud**

A private cloud is dedicated to one organization and not shared with others.

### **16. B) Wireshark**

Wireshark is a powerful tool for packet capture and network troubleshooting.

### **17. B) Define roles and actions during security incidents**

Incident Response Plans guide organizations in handling breaches effectively.

### **18. C) Correlate and analyze security event data**

SIEMs collect, normalize, and analyze logs for threat detection.

### **19. B) Preparation**

Being prepared is the first step to respond quickly and effectively to incidents.

### **20. B) Security log**

Security logs record access attempts, login activity, and authorization events.

### **21. A) NIST CSF**

The NIST Cybersecurity Framework helps manage and reduce cybersecurity risk.

### **22. B) Centralize the management of risk and compliance efforts**

GRC tools help streamline risk, compliance, and policy enforcement.

### **23. A) The level of risk an organization is willing to accept**

Risk appetite defines how much uncertainty an organization is comfortable with.

### **24. A) GDPR**

GDPR mandates breach notifications to individuals within 72 hours.

### **25. A) Identify critical business functions and the impact of disruptions**

BIAs assess how interruptions affect operations.

### **26. A) A generic salutation such as 'Dear Customer'**

Phishing emails often use impersonal greetings to trick recipients.

### **27. A) Internet of Things (IoT) attack**

Smart thermostats and other IoT devices can be exploited if not secured.

### **28. A) Zero-day exploit**

These exploits target unknown vulnerabilities before a patch is available.

### **29. A) Locking the user’s files and demanding payment for a decryption key**

This is the classic behavior of ransomware.

### **30. A) Credential stuffing**

Attackers reuse stolen login credentials across multiple sites.

### **31. B) Secure Sockets Layer (SSL)**

SSL (and its successor TLS) encrypts data during transit.

### **32. B) Ensuring data integrity in transit and at rest**

Data must remain untampered during cloud migration and storage.

### **33. D) Micro-segmentation**

It divides a network into zones for tighter access control.

### **34. B) Enable single sign-on across multiple organizations**

Federated identity systems simplify and centralize authentication.

### **35. A) Provide a secure access point to internal systems for remote users**

A bastion host is hardened and exposed to allow secure access to internal systems.

### **36. A) Chain of custody documentation**

Maintaining evidence integrity is crucial in digital forensics.

### **37. C) User and Entity Behavior Analytics (UEBA)**

UEBA uses machine learning to detect anomalies in behavior.

### **38. A) Password spraying**

This method uses a few passwords across many accounts to avoid lockouts.

### **39. A) Automate and standardize responses to common incidents**

SOAR playbooks streamline and automate security operations.

### **40. B) Security cameras**

Detective controls don't prevent incidents but help identify them afterward.

### **41. C) Identify certificates that are no longer valid**

A CRL lists revoked or expired digital certificates.

### **42. B) AES**

AES is the primary encryption algorithm used in WPA3.

### **43. A) Faster key generation and encryption**

ECC achieves strong encryption with shorter key lengths than RSA.

### **44. B) SFTP**

SFTP encrypts file transfer data for secure communications.

### **45. A) Hashing**

Hashing ensures file integrity by verifying content hasn’t changed.

### **46. C) GDPR**

It protects EU citizens' personal data globally.

### **47. B) Protect personal health information**

HIPAA focuses on safeguarding medical records.

### **48. B) Recovery Time Objective (RTO)**

RTO defines how quickly a system must be restored after a failure.

### **49. B) Identify and classify assets**

Understanding what needs protection comes first in risk assessments.

### **50. A) Penetration testing**

Pen tests simulate real attacks to find and fix vulnerabilities.

### **51. C) Limit the spread of the attack**

Containment stops the incident from spreading across systems.

### **52. B) File Integrity Monitoring (FIM)**

FIM detects unauthorized changes to critical files.

### **53. B) Distributed Denial of Service (DDoS)**

Massive, coordinated traffic floods a service, disrupting availability.

### **54. B) Implementing write-once-read-many (WORM) media**

WORM ensures logs can't be altered after creation.

### **55. B) Review and validate the response plan without live execution**

Tabletop exercises simulate scenarios without affecting real systems.

### **56. B) Implement network segmentation for IoT devices**

Segmenting IoT devices limits exposure from compromised nodes.

### **57. D) SQL injection**

Malicious input modifies SQL queries to extract or manipulate data.

### **58. A) Input validation**

Proper input checks prevent code execution vulnerabilities.

### **59. C) DNS zone transfer**

Zone transfers can expose internal DNS records if misconfigured.

### **60. A) Increase computational difficulty for brute force attacks**

Salting adds randomness, making precomputed hash attacks ineffective.

### **61. B) Provide secure communication over the internet**

TLS encrypts data during transport, preventing interception.

### **62. C) SHA-256**

SHA-256 is currently considered secure and widely used in digital signatures.

### **63. A) It uses a single key for encryption and decryption**

Symmetric encryption is fast and efficient but less scalable.

### **64. A) Advanced Encryption Standard (AES)**

AES secures wireless communications in WPA3.

### **65. C) Recipient’s private key**

Only the recipient's private key can decrypt messages encrypted with their public key.

### **66. B) Simulate an isolated environment to observe malware behavior**

Sandboxes isolate threats to analyze them safely.

### **67. A) VPN**

VPNs secure remote access over public networks.

### **68. B) Context-aware**

Geofencing is a type of context-aware access control using physical location.

### **69. C) Next-generation firewall (NGFW)**

NGFWs inspect traffic at the application layer for deeper visibility.

### **70. B) Ensure only compliant devices access the network**

NAC ensures that only healthy, authorized devices connect.

### **71. B) Protection of financial records**

SOX mandates strict financial data integrity and auditability.

### **72. B) Refusing to engage in high-risk activities**

Avoidance eliminates the risk altogether by not participating.

### **73. D) Open Web Application Security Project**

OWASP publishes the Top Ten most critical web app vulnerabilities.

### **74. B) Prevent sensitive data from leaving the organization**

DLP solutions prevent leaks of sensitive files or information.

### **75. C) HIPAA**

HIPAA requires strong controls like encryption to protect patient data.

### **76. C) Deploy multi-factor authentication (MFA)**

MFA protects against unauthorized access even if passwords are compromised.

### **77. B) Volatility**

Volatility is a memory forensics framework used to analyze RAM dumps.

### **78. A) Containment**

Disconnecting infected systems prevents further spread of malware.

### **79. B) Security logs**

Security logs show login attempts, failures, and access patterns.

### **80. C) Provide detailed instructions for handling specific scenarios**

Runbooks are step-by-step guides for incident handling.

### **81. A) Evil twin**

An evil twin is a rogue wireless access point designed to mimic legitimate ones.

### **82. A) Polymorphic malware**

Polymorphic malware changes its code to evade detection.

### **83. A) Implement input validation**

Input validation is a key defense against API attacks.

### **84. A) Cross-site scripting (XSS)**

XSS injects malicious scripts into trusted websites.

### **85. C) Conducting regular employee awareness training**

Training builds resistance to manipulation and phishing.

### **86. B) Non-repudiation**

Non-repudiation ensures the sender cannot deny sending a message.

### **87. A) Prevent the reuse of session keys**

Perfect Forward Secrecy (PFS) ensures each session uses a unique key.

### **88. A) S/MIME**

S/MIME secures email with digital signatures and encryption.

### **89. A) SHA-256**

SHA-256 is secure and commonly used for document integrity and signing.

### **90. A) Block ciphers encrypt data in fixed-size chunks, while stream ciphers encrypt data bit by bit**

This is the core difference between the two cipher types.

### **91. B) Centralize network control and improve flexibility**

SDN allows dynamic network control through software instead of hardware.

### **92. A) TLS**

TLS protects against man-in-the-middle attacks with encryption and authentication.

### **93. B) Continuous verification of identity and access**

Zero trust means verifying every request, even inside the network.

### **94. C) Intercept and filter web traffic**

Proxy servers inspect, filter, and log web requests.

### **95. A) Enhance application availability and fault tolerance**

Load balancers distribute traffic to ensure uptime and redundancy.

### **96. C) PCI DSS**

PCI DSS focuses on protecting payment card information.

### **97. C) Ensure data is kept for compliance purposes**

Retention policies govern how long data is stored to meet legal needs.

### **98. C) NIST Cybersecurity Framework (CSF)**

NIST CSF emphasizes continuous improvement in cyber maturity.

### **99. B) Annualized Loss Expectancy (ALE)**

ALE helps prioritize risks by calculating expected annual losses.

### **100. B) Secure storage of health records**

HIPAA compliance includes securing electronic health records from breaches.