

Satender Kumar Practice Test 1 - CompTIA Security+ (SY0-701).

1. **Which of the following scenarios best demonstrates the principle of confidentiality?**
 - A) Encrypting sensitive files before transmission
 - B) Detecting unauthorized changes in a document
 - C) Ensuring servers are available during peak hours
 - D) Creating redundant backups of critical data
2. **Which framework provides a structured approach for managing security and risk in an organization?**
 - A) GDPR
 - B) ISO 27001
 - C) COBIT
 - D) PCI DSS
3. **In the CIA triad, availability ensures which of the following?**
 - A) Only authorized users can access data
 - B) Data remains accurate and trustworthy
 - C) Resources are accessible when needed
 - D) Unauthorized users are denied access
4. **Which access control model restricts access based on policies defined by the system administrator?**
 - A) Discretionary Access Control (DAC)
 - B) Role-Based Access Control (RBAC)
 - C) Attribute-Based Access Control (ABAC)
 - D) Mandatory Access Control (MAC)
5. **What does the principle of least privilege ensure?**
 - A) Users have minimal access necessary to perform their tasks
 - B) All users must authenticate with multi-factor authentication
 - C) Data access is monitored continuously
 - D) Privileged accounts are disabled by default
6. **What type of malware disguises itself as legitimate software to gain unauthorized access?**
 - A) Worm
 - B) Rootkit
 - C) Trojan
 - D) Keylogger
7. **Which attack method uses DNS spoofing to redirect users to malicious websites?**
 - A) Pharming
 - B) Phishing
 - C) Shoulder surfing
 - D) Cross-site scripting
8. **Which of the following is an example of a social engineering attack?**
 - A) SQL Injection
 - B) Ransomware attack
 - C) An attacker posing as IT support to obtain user credentials
 - D) A brute force password attack
9. **Which vulnerability allows attackers to execute code remotely on a system?**
 - A) Command injection
 - B) Privilege escalation
 - C) Buffer overflow
 - D) Zero-day exploit
10. **What is the primary goal of implementing a honeypot in a network?**

- A) Detect and log unauthorized access attempts
 - B) Prevent malware infections
 - C) Encrypt sensitive data
 - D) Improve network performance
11. **Which of the following best describes a demilitarized zone (DMZ)?**
- A) A segment of a network used exclusively for storing sensitive data
 - B) A subnet that hosts public-facing services and isolates them from the internal network
 - C) A firewall rule designed to block incoming traffic
 - D) A secure VPN tunnel between two sites
12. **What does micro-segmentation achieve in network security?**
- A) Isolates workloads to reduce the attack surface
 - B) Encrypts all traffic within the network
 - C) Implements zero trust policies across an organization
 - D) Consolidates network traffic for better monitoring
13. **Which of the following devices is primarily used to detect and respond to suspicious network activity?**
- A) Router
 - B) Proxy server
 - C) Intrusion Prevention System (IPS)
 - D) Load balancer
14. **What is the main purpose of a Virtual Private Network (VPN)?**
- A) Enhance wireless connectivity
 - B) Encrypt communications over insecure networks
 - C) Reduce bandwidth usage
 - D) Block unauthorized devices from connecting to the network
15. **Which cloud deployment model is exclusively available to a single organization?**
- A) Public cloud
 - B) Private cloud
 - C) Hybrid cloud
 - D) Community cloud
16. **Which tool is commonly used for packet analysis during a network investigation?**
- A) Nessus
 - B) Wireshark
 - C) Splunk
 - D) Netcat
17. **What is the purpose of an incident response plan?**
- A) Monitor system performance
 - B) Define roles and actions during security incidents
 - C) Enforce compliance with regulatory standards
 - D) Conduct vulnerability scans
18. **Which of the following is a function of a Security Information and Event Management (SIEM) system?**
- A) Perform penetration testing
 - B) Automate software patching
 - C) Correlate and analyze security event data
 - D) Provide real-time endpoint protection
19. **What is the first phase of the incident response process?**
- A) Eradication
 - B) Preparation
 - C) Recovery

- D) Containment
- 20. **Which type of log provides information about user logins and authentication attempts?**
 - A) System log
 - B) Security log
 - C) Application log
 - D) Audit log
- 21. **Which framework is used for assessing and improving critical infrastructure cybersecurity?**
 - A) NIST CSF
 - B) ITIL
 - C) ISO 31000
 - D) COBIT
- 22. **What is the primary benefit of implementing governance, risk, and compliance (GRC) tools?**
 - A) Automate vulnerability scanning
 - B) Centralize the management of risk and compliance efforts
 - C) Improve encryption mechanisms
 - D) Prevent all cyberattacks
- 23. **What does the term "risk appetite" refer to in a security context?**
 - A) The level of risk an organization is willing to accept
 - B) The total number of identified vulnerabilities
 - C) The cost of implementing a risk mitigation strategy
 - D) The likelihood of a threat exploiting a vulnerability
- 24. **Which regulation requires organizations to notify individuals of a data breach?**
 - A) GDPR
 - B) PCI DSS
 - C) HIPAA
 - D) ISO 27001
- 25. **What is the goal of a business impact analysis (BIA)?**
 - A) Identify critical business functions and the impact of disruptions
 - B) Define roles in an incident response team
 - C) Assess the effectiveness of security policies
 - D) Calculate the cost of implementing new technology
- 26. **Which of the following is an indicator of a phishing attempt in an email?**
 - A) A generic salutation such as "Dear Customer"
 - B) The presence of a company logo
 - C) A correctly spelled domain name in the sender's address
 - D) A secure HTTPS link in the email body
- 27. **An attacker exploits a vulnerability in a smart thermostat connected to the network. Which type of attack is this?**
 - A) Internet of Things (IoT) attack
 - B) Distributed Denial of Service (DDoS) attack
 - C) Social engineering attack
 - D) SQL injection
- 28. **What technique is used by attackers to exploit an unpatched software vulnerability before the vendor releases a fix?**
 - A) Zero-day exploit
 - B) Cross-site scripting
 - C) Privilege escalation
 - D) DLL injection
- 29. **Which of the following is an example of a ransomware attack?**
 - A) Locking the user's files and demanding payment for a decryption key

- B) Exploiting a vulnerability to execute unauthorized code
 - C) Monitoring user activity through a spyware program
 - D) Redirecting traffic from a legitimate site to a malicious one
30. **A malicious actor uses stolen credentials to log into an online banking platform. What type of attack is this?**
- A) Credential stuffing
 - B) Replay attack
 - C) Brute force attack
 - D) Keylogger attack
31. **Which security measure ensures data transmitted between two systems is encrypted end-to-end?**
- A) Virtual Private Network (VPN)
 - B) Secure Sockets Layer (SSL)
 - C) Multi-factor authentication (MFA)
 - D) Network Access Control (NAC)
32. **An organization is migrating critical applications to the cloud. Which security challenge is most relevant?**
- A) Managing on-premises firewalls
 - B) Ensuring data integrity in transit and at rest
 - C) Monitoring legacy systems
 - D) Installing endpoint antivirus software
33. **Which of the following technologies is most effective in segmenting and isolating different workloads within a cloud environment?**
- A) VLANs
 - B) Zero Trust Architecture
 - C) Firewalls
 - D) Micro-segmentation
34. **What is the primary goal of implementing a federated identity management system?**
- A) Encrypt sensitive data at rest
 - B) Enable single sign-on across multiple organizations
 - C) Strengthen multi-factor authentication processes
 - D) Reduce the attack surface in hybrid environments
35. **A company deploys a bastion host in its DMZ. What is the main purpose of this host?**
- A) Provide a secure access point to internal systems for remote users
 - B) Encrypt all inbound and outbound traffic
 - C) Act as a firewall for the internal network
 - D) Host public-facing applications securely
36. **Which of the following is the most critical first step when conducting a forensic investigation?**
- A) Chain of custody documentation
 - B) Removing the compromised system from the network
 - C) Backing up log files
 - D) Analyzing memory and disk images
37. **What type of solution uses machine learning to detect anomalies in user behavior and flag potential security threats?**
- A) Intrusion Detection System (IDS)
 - B) Endpoint Detection and Response (EDR)
 - C) User and Entity Behavior Analytics (UEBA)
 - D) Vulnerability Scanner
38. **An analyst is reviewing logs and notices repeated login attempts from multiple IP addresses. What is the likely attack method?**

- A) Password spraying
 - B) Phishing
 - C) SQL injection
 - D) Privilege escalation
39. **What is the primary purpose of using playbooks in a Security Orchestration, Automation, and Response (SOAR) platform?**
- A) Automate and standardize responses to common incidents
 - B) Generate compliance reports for auditors
 - C) Improve endpoint protection capabilities
 - D) Conduct vulnerability assessments
40. **Which of the following is considered a detective control?**
- A) Firewall rules
 - B) Security cameras
 - C) Data encryption
 - D) Antivirus software
41. **What is the purpose of a certificate revocation list (CRL) in a Public Key Infrastructure (PKI)?**
- A) Validate a certificate's authenticity
 - B) Distribute public keys to users
 - C) Identify certificates that are no longer valid
 - D) Encrypt email communications
42. **Which encryption algorithm is used in Wi-Fi Protected Access 3 (WPA3)?**
- A) RSA
 - B) AES
 - C) SHA-256
 - D) Blowfish
43. **What is the main advantage of elliptic curve cryptography (ECC) over traditional algorithms like RSA?**
- A) Faster key generation and encryption
 - B) Requires longer keys for the same security level
 - C) Uses symmetric key encryption
 - D) Focuses on hashing operations
44. **A company needs to securely transfer large amounts of sensitive data between systems. Which protocol should they use?**
- A) SSH
 - B) SFTP
 - C) HTTP
 - D) FTP
45. **Which cryptographic method ensures the integrity of a file during transfer?**
- A) Hashing
 - B) Asymmetric encryption
 - C) Symmetric encryption
 - D) Tokenization
46. **Which of the following regulations requires companies to protect EU citizens' personal data, regardless of where the company is located?**
- A) PCI DSS
 - B) HIPAA
 - C) GDPR
 - D) SOX
47. **What is the primary purpose of the Health Insurance Portability and Accountability Act (HIPAA)?**

- A) Secure financial data
 - B) Protect personal health information
 - C) Govern cybersecurity frameworks
 - D) Enforce zero-trust policies
48. **Which of the following metrics is used to determine the time allowed to recover a system after a failure?**
- A) Recovery Point Objective (RPO)
 - B) Recovery Time Objective (RTO)
 - C) Mean Time Between Failures (MTBF)
 - D) Maximum Tolerable Downtime (MTD)
49. **A security manager is assessing the risk level of a new cloud application. What is the FIRST step they should take?**
- A) Perform a vulnerability scan
 - B) Identify and classify assets
 - C) Conduct a business impact analysis
 - D) Review compliance requirements
50. **Which type of assessment involves simulating real-world attacks to test system defenses?**
- A) Penetration testing
 - B) Vulnerability scanning
 - C) Risk assessment
 - D) Patch management
51. **During an incident response, what is the primary goal of the containment phase?**
- A) Identify the root cause of the incident
 - B) Eradicate the threat from the environment
 - C) Limit the spread of the attack
 - D) Notify regulatory authorities
52. **Which of the following tools would an analyst use to detect unauthorized changes to files on a server?**
- A) SIEM
 - B) File Integrity Monitoring (FIM)
 - C) Vulnerability scanner
 - D) Network Access Control (NAC)
53. **A company's DNS server is experiencing an overwhelming number of requests. Logs indicate requests are coming from multiple sources simultaneously. Which type of attack is this?**
- A) DNS spoofing
 - B) Distributed Denial of Service (DDoS)
 - C) DNS amplification
 - D) Man-in-the-middle
54. **Which logging practice ensures that log files are protected from tampering after they are created?**
- A) Rotating logs regularly
 - B) Implementing write-once-read-many (WORM) media
 - C) Encrypting log files during storage
 - D) Storing logs on a network share
55. **What is the purpose of a tabletop exercise in incident response planning?**
- A) Simulate a real attack scenario to test systems
 - B) Review and validate the response plan without live execution
 - C) Conduct penetration testing on a network
 - D) Generate automated incident response playbooks

56. **An attacker uses a compromised IoT device as part of a botnet to perform a DDoS attack. What is the best mitigation?**
- A) Deploy a Web Application Firewall (WAF)
 - B) Implement network segmentation for IoT devices
 - C) Install antivirus software on IoT devices
 - D) Conduct regular penetration tests
57. **Which type of vulnerability involves user input that modifies SQL queries to gain unauthorized database access?**
- A) Buffer overflow
 - B) Cross-site scripting
 - C) Command injection
 - D) SQL injection
58. **What technique prevents an attacker from exploiting a memory corruption vulnerability in an application?**
- A) Input validation
 - B) Security patching
 - C) Data encryption
 - D) Secure boot
59. **Which of the following methods can attackers use to covertly gather data about a target network?**
- A) Ping sweep
 - B) ARP poisoning
 - C) DNS zone transfer
 - D) MAC spoofing
60. **What is the main purpose of using salting in password security?**
- A) Increase computational difficulty for brute force attacks
 - B) Enable multi-factor authentication
 - C) Encrypt stored passwords
 - D) Prevent dictionary attacks using precomputed hashes
61. **What is the primary purpose of Transport Layer Security (TLS)?**
- A) Encrypt email communications
 - B) Provide secure communication over the internet
 - C) Authenticate users during login
 - D) Detect unauthorized file access
62. **Which of the following hashing algorithms is considered secure for modern cryptographic use?**
- A) MD5
 - B) SHA-1
 - C) SHA-256
 - D) RC4
63. **What is the key characteristic of symmetric encryption?**
- A) It uses a single key for encryption and decryption
 - B) It relies on public-private key pairs
 - C) It provides digital signatures for data integrity
 - D) It supports blockchain operations
64. **Which cryptographic protocol is used to secure wireless communications under WPA3?**
- A) Advanced Encryption Standard (AES)
 - B) Diffie-Hellman Key Exchange
 - C) RSA
 - D) Elliptic Curve Digital Signature Algorithm (ECDSA)

65. **A user receives an email encrypted using a recipient's public key. What is required to decrypt it?**
- A) Sender's private key
 - B) Sender's public key
 - C) Recipient's private key
 - D) Recipient's public key
66. **What is the primary function of a sandbox in malware analysis?**
- A) Protect sensitive data from malware
 - B) Simulate an isolated environment to observe malware behavior
 - C) Prevent phishing attacks
 - D) Encrypt malware signatures
67. **Which technology enables secure communication between branch offices over the internet?**
- A) VPN
 - B) Firewall
 - C) DNSSEC
 - D) SIEM
68. **An organization implements geofencing to restrict access to certain resources. What type of access control is this?**
- A) Role-based
 - B) Context-aware
 - C) Discretionary
 - D) Mandatory
69. **Which type of firewall inspects traffic at the application layer?**
- A) Packet-filtering firewall
 - B) Stateful firewall
 - C) Next-generation firewall (NGFW)
 - D) Circuit-level gateway
70. **What is the purpose of a Network Access Control (NAC) solution?**
- A) Monitor and log network traffic
 - B) Ensure only compliant devices access the network
 - C) Detect and block phishing emails
 - D) Encrypt data transmitted over the network
71. **What does the Sarbanes-Oxley Act (SOX) primarily address?**
- A) Data breach notification requirements
 - B) Protection of financial records
 - C) Safeguarding health information
 - D) Cross-border data transfers
72. **Which of the following is an example of risk avoidance?**
- A) Purchasing cybersecurity insurance
 - B) Refusing to engage in high-risk activities
 - C) Mitigating risk through technical controls
 - D) Accepting residual risk
73. **Which organization publishes the OWASP Top Ten vulnerabilities?**
- A) ISO
 - B) NIST
 - C) (ISC)²
 - D) Open Web Application Security Project
74. **What is the purpose of a Data Loss Prevention (DLP) solution?**
- A) Encrypt data stored on servers
 - B) Prevent sensitive data from leaving the organization

- C) Monitor user activity across the network
- D) Enforce user access policies

75. **Which regulation requires encryption of patient health information to ensure confidentiality?**

- A) GDPR
 - B) PCI DSS
 - C) HIPAA
 - D) FISMA
-

76. **An analyst finds that multiple accounts were compromised due to weak passwords. What is the best remediation step?**

- A) Implement account lockout policies
- B) Require users to update passwords regularly
- C) Deploy multi-factor authentication (MFA)
- D) Conduct security awareness training

77. **Which tool would you use to analyze malicious activity in system memory?**

- A) Wireshark
- B) Volatility
- C) Nessus
- D) Splunk

78. **During an incident, the security team disconnects an infected machine from the network. Which incident response step does this represent?**

- A) Containment
- B) Eradication
- C) Recovery
- D) Preparation

79. **Which log type is essential for identifying the source of unauthorized login attempts?**

- A) Firewall logs
- B) Security logs
- C) Application logs
- D) DNS logs

80. **What is the main purpose of a runbook in incident response?**

- A) Document roles in the incident response team
- B) Automate repetitive tasks during incidents
- C) Provide detailed instructions for handling specific scenarios
- D) Identify vulnerabilities in the network

81. **An attacker uses a fake access point to intercept sensitive information during a wireless session. What is this attack called?**

- A) Evil twin
- B) Rogue AP
- C) Bluejacking
- D) Packet sniffing

82. **What type of malware modifies itself to avoid detection by antivirus software?**

- A) Polymorphic malware
- B) Rootkit
- C) Spyware
- D) Logic bomb

83. **An attacker gains access to a system by exploiting a weak API. What is the best preventive control?**

- A) Implement input validation

- B) Encrypt API traffic
 - C) Monitor API usage with a SIEM
 - D) Use TLS for all communications
84. **What technique involves sending malicious scripts to a trusted website that executes in the user's browser?**
- A) Cross-site scripting (XSS)
 - B) SQL injection
 - C) Command injection
 - D) Buffer overflow
85. **Which of the following would best protect against social engineering attacks?**
- A) Enforcing strong password policies
 - B) Implementing email filtering solutions
 - C) Conducting regular employee awareness training
 - D) Deploying endpoint detection and response (EDR)
86. **Which cryptographic concept ensures that a sender cannot deny sending a message?**
- A) Encryption
 - B) Non-repudiation
 - C) Integrity
 - D) Authentication
87. **What is the purpose of perfect forward secrecy (PFS) in encryption protocols?**
- A) Prevent the reuse of session keys
 - B) Ensure data confidentiality during transmission
 - C) Support large-scale certificate management
 - D) Detect unauthorized modifications
88. **A company needs to implement a secure email solution that verifies the sender's identity and ensures message integrity. Which protocol should they use?**
- A) S/MIME
 - B) POP3
 - C) IMAP
 - D) SMTP
89. **Which hashing algorithm is suitable for digitally signing documents?**
- A) SHA-256
 - B) MD5
 - C) RC4
 - D) AES
90. **What is the primary difference between block and stream ciphers?**
- A) Block ciphers encrypt data in fixed-size chunks, while stream ciphers encrypt data bit by bit
 - B) Block ciphers use symmetric keys, and stream ciphers use asymmetric keys
 - C) Block ciphers are faster for real-time data encryption
 - D) Stream ciphers offer better support for file encryption
91. **What is the purpose of implementing software-defined networking (SDN) in a data center?**
- A) Encrypt all network traffic
 - B) Centralize network control and improve flexibility
 - C) Prevent unauthorized access to physical devices
 - D) Deploy microservices securely
92. **Which of the following technologies would best protect against man-in-the-middle attacks?**
- A) TLS
 - B) DNSSEC
 - C) WPA2

- D) SIEM
93. **An organization is considering the zero-trust model. What is a key requirement for this framework?**
- A) Implicit trust within internal networks
 - B) Continuous verification of identity and access
 - C) Relying solely on perimeter firewalls
 - D) Storing all data on-premises
94. **What is the primary function of a proxy server in a secure network?**
- A) Block malware downloads
 - B) Cache frequently accessed resources
 - C) Intercept and filter web traffic
 - D) Monitor network bandwidth usage
95. **Which of the following is a benefit of using a load balancer in a web application environment?**
- A) Enhance application availability and fault tolerance
 - B) Encrypt all web application traffic
 - C) Detect and block SQL injection attempts
 - D) Ensure compliance with GDPR
96. **Which regulation is primarily concerned with protecting cardholder data?**
- A) GDPR
 - B) HIPAA
 - C) PCI DSS
 - D) FISMA
97. **What is the goal of implementing a retention policy for sensitive data?**
- A) Reduce storage costs
 - B) Limit access to data
 - C) Ensure data is kept for compliance purposes
 - D) Prevent unauthorized data transfers
98. **Which framework emphasizes the assessment and improvement of cybersecurity maturity in critical infrastructure?**
- A) ISO 27001
 - B) COBIT
 - C) NIST Cybersecurity Framework (CSF)
 - D) ITIL
99. **What is a common metric used in risk management to prioritize mitigation efforts?**
- A) Recovery Point Objective (RPO)
 - B) Annualized Loss Expectancy (ALE)
 - C) Recovery Time Objective (RTO)
 - D) Residual Risk
100. **An auditor is reviewing an organization's compliance with HIPAA. Which of the following would most likely be assessed?**
- A) Encryption of payment card information
 - B) Secure storage of health records
 - C) Implementation of firewall rules
 - D) Password complexity policies