Satender KumarPractice Test 2 - CompTIA Security+ (SY0-701).

1. **A security team is investigating unauthorized access to an internal database. The logs reveal that an attacker used credentials stolen from an employee. Which mitigation would best prevent this type of attack in the future?**
    - A) Deploying endpoint detection and response (EDR) solutions
    - B) Enforcing multi-factor authentication (MFA)
    - C) Installing a host-based intrusion detection system (HIDS)
    - D) Implementing network segmentation
2. **Which security practice ensures that a developer's new code does not introduce vulnerabilities to an application?**
    - A) Continuous monitoring
    - B) Secure coding practices
    - C) Input sanitization
    - D) Patch management
3. **An organization implements a full packet capture solution to analyze network traffic. Which scenario would most benefit from this capability?**
    - A) Identifying malware signatures in files
    - B) Investigating the scope of a data breach
    - C) Blocking phishing attempts in real time
    - D) Monitoring compliance with privacy regulations
4. **During a penetration test, the tester exploits a vulnerability that allows arbitrary code execution. What is the next recommended step according to ethical testing guidelines?**
    - A) Escalate privileges on the compromised system
    - B) Document the vulnerability and report it immediately
    - C) Continue testing the system for other vulnerabilities
    - D) Install monitoring software on the target system
5. **An organization uses a third-party cloud provider for hosting its applications. What is the most effective way to ensure the security of its data in this environment?**
    - A) Encrypt data both in transit and at rest
    - B) Use a dedicated public IP address for cloud resources
    - C) Require all users to connect via a VPN
    - D) Perform regular penetration tests on the cloud infrastructure
6. **Which of the following would indicate a successful DNS poisoning attack?**
    - A) Users are redirected to a malicious website when accessing legitimate URLs
    - B) A network experiences an increase in unsolicited ARP traffic
    - C) Hosts within the network cannot resolve external domain names
    - D) Internal DNS queries are being logged without authorization
7. **An attacker exploits a web application by injecting malicious JavaScript code into an input field. What is the best countermeasure to prevent this type of attack?**
    - A) Enforce strict input validation on all user input
    - B) Implement server-side encryption of user data
    - C) Restrict access to the application’s API endpoints
    - D) Require multi-factor authentication for all users
8. **A user reports that their computer screen suddenly displays a message demanding payment in exchange for file access. What immediate action should the incident response team take?**
    - A) Isolate the affected device from the network
    - B) Power off the device to prevent further damage
    - C) Pay the ransom to recover the files quickly

    - D) Restore the files from a recent backup
9. **Which of the following technologies is most effective in detecting insider threats within an organization?**
    - A) Endpoint Detection and Response (EDR)
    - B) User and Entity Behavior Analytics (UEBA)
    - C) Data Loss Prevention (DLP) systems
    - D) Intrusion Prevention Systems (IPS)
10. **An organization detects unusual outbound traffic to a known malicious IP address. What is the most likely explanation?**
    - A) A denial-of-service (DoS) attack
    - B) A compromised system sending data to a command-and-control (C2) server
    - C) An employee bypassing corporate security controls
    - D) A misconfigured firewall rule allowing outbound traffic
11. **A company implements data-at-rest encryption for its database servers. What additional step should they take to ensure the encryption is effective?**
    - A) Use key rotation policies to manage encryption keys
    - B) Encrypt backups stored offsite
    - C) Ensure the database has role-based access controls (RBAC)
    - D) Use symmetric keys for faster encryption
12. **An attacker successfully performs a SQL injection on a company's website. What is the most likely root cause?**
    - A) Lack of a web application firewall
    - B) Insecure input handling in the application
    - C) Absence of database encryption
    - D) Weak passwords on the database server
13. **An attacker uses an email claiming to be from IT support to obtain a user's login credentials. What type of attack is this?**
    - A) Whaling
    - B) Spear phishing
    - C) Vishing
    - D) Pretexting
14. **What is the primary benefit of using containerization for application deployment?**
    - A) Encrypting application data by default
    - B) Isolating applications to reduce the impact of a compromise
    - C) Allowing real-time monitoring of all application code
    - D) Preventing zero-day vulnerabilities
15. **During a review of a cloud infrastructure, a security engineer discovers excessive permissions granted to several user accounts. What is the best course of action?**
    - A) Implement least privilege access
    - B) Require users to rotate passwords every 30 days
    - C) Configure network segmentation to isolate sensitive resources
    - D) Enable logging to monitor all user activity
16. **A company uses a VPN for remote employees. During a security review, it is noted that several VPN accounts are being used simultaneously from different locations. What should be implemented to prevent this?**

- A) Split tunneling
- B) Multi-factor authentication
- C) Context-aware access control
- D) Single sign-on

17. **Which type of malware installs a hidden backdoor to allow unauthorized remote access?**

- A) Ransomware

- B) Rootkit
- C) Spyware
- D) Adware

18. **A security analyst observes outbound traffic to a non-standard port from a high-value asset. What is the most appropriate action?**
- A) Block the port at the firewall and investigate further
- B) Perform a full packet capture of the traffic
- C) Notify the system owner and take no action
- D) Restart the system to terminate the connection

19. **An attacker embeds malicious code in an image file, which executes when the image is opened. What type of attack is this?**
- A) Steganography
- B) Cross-site scripting (XSS)
- C) Logic bomb
- D) Watering hole attack

20. **What is the primary purpose of tokenization in securing sensitive information?**
- A) Encrypt data for secure storage
- B) Replace sensitive data with non-sensitive equivalents
- C) Enable secure multi-factor authentication
- D) Hash sensitive information for integrity

21. **Which of the following tools would best identify vulnerabilities in an application before deployment?**
- A) Static Application Security Testing (SAST)
- B) Security Information and Event Management (SIEM)
- C) Network vulnerability scanner
- D) Intrusion detection system

22. **An attacker redirects a victim to a malicious website by altering DNS records. What is this attack called?**
- A) ARP poisoning
- B) DNS spoofing
- C) IP spoofing
- D) Smishing

23. **What is the best way to defend against brute force attacks on an organization's login portal?**
- A) Require CAPTCHA for all login attempts
- B) Enforce account lockout after a number of failed attempts
- C) Deploy a firewall with strict access control
- D) Implement email-based two-factor authentication

24. **A company's employees use public Wi-Fi for accessing sensitive corporate data. What is the most effective security measure?**
- A) Enforce VPN usage
- B) Block public Wi-Fi access for corporate devices
- C) Use MAC address filtering
- D) Disable file sharing

25. **Which of the following would mitigate the risk of an attacker using a USB device to install malware on corporate systems?**
- A) Enable Secure Boot
- B) Implement endpoint device control policies
- C) Deploy anti-malware on all systems
- D) Enforce email attachment filtering

26. **What is the primary benefit of using security groups in a cloud environment?**

- A) Encrypt traffic between virtual machines
- B) Define and enforce granular access controls
- C) Automate firewall rule configurations
- D) Provide zero-trust network access

27. **An attacker successfully exploits a buffer overflow in an application. What is the most likely goal of this attack?**
- A) Execute arbitrary code
- B) Conduct a man-in-the-middle attack
- C) Steal sensitive data
- D) Install ransomware

28. **An organization deploys honeypots in its network. What is the primary purpose of this strategy?**
- A) Enhance user authentication security
- B) Divert attackers and study their behavior
- C) Encrypt sensitive data in transit
- D) Accelerate vulnerability scans

29. **A company implements a log retention policy requiring logs to be stored for 7 years. What should the company do to ensure compliance?**
- A) Encrypt logs before archiving
- B) Use write-once-read-many (WORM) storage
- C) Store logs in the cloud for cost efficiency
- D) Automate log rotation every 30 days

30. **Which type of cryptographic key should be used for establishing secure communications in a public network?**
- A) Symmetric key
- B) Asymmetric key pair
- C) Pre-shared key
- D) One-time pad

31. **A security analyst is reviewing logs and notices that sensitive files were accessed outside normal business hours. What is the most likely type of attack?**
- A) Insider threat
- B) Credential stuffing
- C) Privilege escalation
- D) Malware infection

32. **Which of the following techniques would best protect against privilege escalation attacks?**
- A) Use secure coding practices
- B) Enforce multi-factor authentication
- C) Implement role-based access control (RBAC)
- D) Configure firewalls to block unauthorized traffic

33. **What is the main function of a bastion host?**
- A) Detect network intrusions
- B) Host public-facing services securely
- C) Provide backup for critical servers
- D) Encrypt sensitive communications

34. **Which attack involves sending specially crafted packets to crash a network device?**
- A) SYN flood
- B) Ping of Death
- C) Teardrop attack
- D) Replay attack

35. **What is the main reason for implementing micro-segmentation in a network?**
- A) Simplify network routing

- B) Isolate sensitive systems from potential threats
- C) Improve firewall efficiency
- D) Enhance data encryption during transmission

36. **A user reports receiving an email from their bank asking for login credentials. What type of attack is this?**
- A) Whaling
- B) Spear phishing
- C) Phishing
- D) Vishing

37. **What is the best strategy to minimize risk when deploying a new application in production?**
- A) Use automated vulnerability scanning during development
- B) Conduct a penetration test before deployment
- C) Encrypt all application data
- D) Perform real-time monitoring during launch

38. **Which of the following describes a defense-in-depth approach?**
- A) Multiple layers of security controls to protect assets
- B) Encrypting sensitive data at rest and in transit
- C) Implementing firewalls at every network layer
- D) Using intrusion detection and prevention systems

39. **What is the primary role of a Security Orchestration, Automation, and Response (SOAR) platform?**
- A) Correlate security events in real time
- B) Automate incident response workflows
- C) Prevent ransomware attacks
- D) Analyze vulnerabilities in real-time

40. **An attacker exploits a vulnerability in a third-party library used by an application. What is the best way to mitigate this risk?**
- A) Implement a web application firewall
- B) Conduct regular code reviews
- C) Use dependency scanning tools
- D) Update the application to remove the library

41. **Which attack involves intercepting and altering communications between two parties without their knowledge?**
- A) DNS poisoning
- B) Man-in-the-middle (MITM)
- C) Phishing
- D) Replay attack

42. **An organization implements port security on its switches. What does this configuration achieve?**
- A) Blocks unauthorized devices from connecting to the network
- B) Monitors traffic for malicious activity
- C) Encrypts all communications within the local network
- D) Enhances physical security of network hardware

43. **A company wants to prevent unauthorized access to physical servers in its data center. Which control would be most effective?**
- A) Biometric authentication at entry points
- B) Role-based access control (RBAC)
- C) Network Access Control (NAC)
- D) Enforcing strong passwords for admin accounts

44. **What is the primary goal of implementing a Web Application Firewall (WAF)?**

- A) Prevent denial-of-service attacks on the network
- B) Block malicious HTTP/S requests to web applications
- C) Monitor and log all outbound traffic
- D) Encrypt sensitive web communications

45. **An organization implements a geofencing policy to restrict access to certain systems. Which type of access control does this represent?**
- A) Role-based
- B) Context-aware
- C) Mandatory
- D) Discretionary

46. **What is the best defense against SQL injection attacks?**
- A) Enforcing strong password policies
- B) Encrypting sensitive database records
- C) Using prepared statements with parameterized queries
- D) Implementing multifactor authentication

47. **A security analyst is tasked with identifying advanced threats within a network. Which tool should they use?**
- A) SIEM with threat intelligence integration
- B) File integrity monitoring
- C) Firewall access logs
- D) Open-source vulnerability scanners

48. **What is the purpose of using hashing in digital signatures?**
- A) Encrypt the original data
- B) Verify the integrity of the message
- C) Provide confidentiality for the communication
- D) Generate public-private key pairs

49. **An attacker floods a target network with ICMP packets. What type of attack is this?**
- A) Distributed Denial of Service (DDoS)
- B) Ping flood
- C) SYN flood
- D) Man-in-the-middle

50. **Which type of malware relies on encryption to make data inaccessible until a ransom is paid?**
- A) Worm
- B) Ransomware
- C) Spyware
- D) Trojan

51. **What is the primary benefit of using public key infrastructure (PKI) in an organization?**
- A) Centralize password management
- B) Ensure data integrity and authentication
- C) Encrypt all email communications
- D) Monitor user activity across the network

52. **Which of the following actions should be taken first during the eradication phase of incident response?**
- A) Restore data from backups
- B) Identify and remove the root cause
- C) Conduct a root cause analysis
- D) Notify stakeholders about the incident

53. **A security analyst notices unusual activity from a user account accessing multiple systems simultaneously. What is the most likely explanation?**
- A) Insider threat

- B) Credential compromise
- C) Application vulnerability
- D) Privilege escalation

54. **What is the main purpose of implementing role-based access control (RBAC)?**
- A) Reduce administrative overhead for permissions management
- B) Encrypt sensitive files and communications
- C) Monitor and log all user activities
- D) Allow dynamic access changes based on context

55. **Which cryptographic method ensures that plaintext cannot be recovered even if the ciphertext is intercepted?**
- A) Encryption
- B) Hashing
- C) Salting
- D) Tokenization

56. **An attacker exploits a known vulnerability in a company's software. What is the best preventive measure?**
- A) Conduct regular vulnerability scanning and patch management
- B) Implement a web application firewall (WAF)
- C) Use strong passwords for all accounts
- D) Deploy multi-factor authentication

57. **Which type of control is a warning banner displayed on a login screen?**
- A) Deterrent control
- B) Detective control
- C) Preventive control
- D) Compensating control

58. **A compromised IoT device in a smart factory was used to pivot to other devices. What is the best security measure to prevent this?**
- A) Implement micro-segmentation for IoT devices
- B) Enforce role-based access control
- C) Monitor traffic using an intrusion detection system
- D) Use symmetric encryption for IoT communications

59. **What is the primary advantage of using a cloud-based SIEM solution over an on-premises SIEM?**
- A) Reduced latency for local events
- B) Improved scalability and centralized management
- C) Simplified integration with endpoint devices
- D) Enhanced encryption for log files

60. **Which technique best protects against rainbow table attacks?**
- A) Salting passwords before hashing
- B) Implementing account lockout policies
- C) Encrypting user credentials during transmission
- D) Using multifactor authentication

61. **Which of the following best defines steganography?**
- A) Encrypting data in transit
- B) Hiding data within other files or media
- C) Obfuscating code to prevent reverse engineering
- D) Using hashing to verify data integrity

62. **What is the purpose of a certificate signing request (CSR) in PKI?**
- A) Request a digital certificate from a certificate authority (CA)
- B) Authenticate a user's identity to the network
- C) Verify the integrity of encrypted data

- D) Secure communications between systems

63. **A company is planning to deploy Zero Trust Architecture. What is a key requirement for this model?**
- A) Implicit trust within internal networks
- B) Continuous verification of users and devices
- C) Use of role-based access controls exclusively
- D) Encrypting all traffic to the cloud

64. **An attacker uses a compromised email account to send phishing emails to internal employees. What type of attack is this?**
- A) Impersonation
- B) Business Email Compromise (BEC)
- C) Whaling
- D) Pretexting

65. **What is the primary purpose of a vulnerability scan?**
- A) Detect and exploit security weaknesses
- B) Identify potential security gaps in a system
- C) Test the effectiveness of an incident response plan
- D) Evaluate compliance with regulatory frameworks

66. **An attacker successfully alters a configuration file on a server without proper authorization. Which security principle has been violated?**
- A) Availability
- B) Integrity
- C) Confidentiality
- D) Non-repudiation

67. **What is the best method to securely transmit confidential information over the internet?**
- A) Secure Sockets Layer (SSL)
- B) Virtual Private Network (VPN)
- C) File Transfer Protocol (FTP)
- D) Simple Mail Transfer Protocol (SMTP)

68. **What is the primary goal of implementing an intrusion prevention system (IPS) in a network?**
- A) Detect and log malicious activity
- B) Block identified threats in real-time
- C) Encrypt network communications
- D) Monitor bandwidth usage

69. **A security analyst identifies unusual outbound traffic from a database server. What should be the analyst's next step?**
- A) Isolate the server from the network
- B) Notify the database administrator
- C) Conduct a vulnerability scan on the server
- D) Disable all user accounts temporarily

70. **Which of the following mitigates the risk of privilege escalation attacks?**
- A) Implement multi-factor authentication
- B) Enforce least privilege policies
- C) Perform regular penetration testing
- D) Use a web application firewall

71. **A company's email system was compromised due to a phishing attack. Which step should be prioritized during the response process?**
- A) Notify affected users
- B) Analyze the malicious email headers
- C) Block the sender's email address

- D) Revoke compromised credentials

72. **What is the purpose of security labels in mandatory access control (MAC)?**
- A) Identify and classify system vulnerabilities
- B) Enforce access policies based on data classification
- C) Assign user roles dynamically based on context
- D) Monitor access attempts in real-time

73. **An attacker uses a public Wi-Fi network to intercept unencrypted web traffic. Which attack type is this?**
- A) ARP poisoning
- B) Evil twin
- C) Packet sniffing
- D) Man-in-the-middle

74. **A compromised device is communicating with a known command-and-control (C2) server. What is the most likely explanation?**
- A) A distributed denial-of-service (DDoS) attack
- B) Malware infection
- C) Credential theft
- D) Insider threat

75. **What is the best way to protect API endpoints from exploitation?**
- A) Require authentication for all API calls
- B) Deploy static application security testing (SAST) tools
- C) Use multi-factor authentication for developers
- D) Block traffic from public IP addresses

76. **Which cryptographic protocol is used to secure web traffic in HTTPS?**
- A) TLS
- B) RSA
- C) AES
- D) SHA

77. **A user receives a phone call from someone claiming to be IT support and requesting their login credentials. What type of attack is this?**
- A) Smishing
- B) Pretexting
- C) Vishing
- D) Impersonation

78. **An attacker exploits a zero-day vulnerability in a company's software. What is the best way to address this risk in the future?**
- A) Conduct real-time monitoring
- B) Implement endpoint detection and response (EDR) solutions
- C) Perform static code analysis on new applications
- D) Maintain a robust patch management process

79. **Which technology uses behavioral analysis to detect anomalies in user activities?**
- A) Security Information and Event Management (SIEM)
- B) User and Entity Behavior Analytics (UEBA)
- C) Intrusion Detection System (IDS)
- D) Vulnerability scanner

80. **A company's IT team wants to limit access to a sensitive database based on specific attributes such as user location and device type. Which access control model should they implement?**
- A) Attribute-Based Access Control (ABAC)
- B) Discretionary Access Control (DAC)
- C) Role-Based Access Control (RBAC)

- D) Mandatory Access Control (MAC)

81. **Which action best protects against credential stuffing attacks?**
- A) Enforce complex password policies
- B) Implement rate limiting on login attempts
- C) Use secure hashing algorithms for stored passwords
- D) Monitor access logs for anomalies

82. **What is the primary purpose of using a demilitarized zone (DMZ) in network design?**
- A) Prevent malware infections in internal systems
- B) Isolate public-facing servers from the internal network
- C) Monitor and log all inbound traffic
- D) Encrypt sensitive communications

83. **Which vulnerability allows attackers to inject malicious code during user input to manipulate a web application?**
- A) Cross-site scripting (XSS)
- B) Directory traversal
- C) SQL injection
- D) Command injection

84. **A company implements a network access control (NAC) solution. What is its primary function?**
- A) Detect and block phishing emails
- B) Prevent unauthorized devices from accessing the network
- C) Encrypt all internal communications
- D) Monitor user activities for anomalies

85. **What is the best way to ensure that logs remain tamper-proof?**
- A) Encrypt all logs before storage
- B) Use write-once-read-many (WORM) media
- C) Store logs in a cloud environment
- D) Automate log rotation every 24 hours

86. **Which type of malware executes its payload when specific conditions are met?**
- A) Trojan
- B) Logic bomb
- C) Worm
- D) Keylogger

87. **What is the main advantage of elliptic curve cryptography (ECC) over RSA?**
- A) Faster encryption and decryption
- B) Shorter key lengths with equivalent security
- C) Easier key management
- D) Greater resistance to brute-force attacks

88. **What is the purpose of conducting a business impact analysis (BIA)?**
- A) Identify and prioritize critical business processes
- B) Perform a gap analysis of security controls
- C) Test the effectiveness of incident response plans
- D) Establish a disaster recovery budget

89. **Which practice helps ensure data integrity during file transfers?**
- A) Using hashing algorithms
- B) Encrypting the file before transfer
- C) Deploying a secure file transfer protocol
- D) Performing periodic audits

90. **An attacker attempts to exploit a vulnerability in the transport layer of a network. What type of security control would be most effective?**
- A) Web Application Firewall (WAF)

- B) Intrusion Prevention System (IPS)
- C) Secure Sockets Layer (SSL)/TLS
- D) Network Access Control (NAC)

91. **What is the primary purpose of using multifactor authentication (MFA)?**
- A) Encrypt sensitive data at rest
- B) Protect against unauthorized access by requiring multiple forms of verification
- C) Ensure secure data transfer over the network
- D) Prevent phishing attempts

92. **An organization notices repeated failed login attempts from multiple IP addresses. What is the most likely type of attack?**
- A) Password spraying
- B) Phishing
- C) SQL injection
- D) Insider threat

93. **Which of the following is the best way to secure containers in a production environment?**
- A) Use a host-based intrusion prevention system
- B) Implement image scanning to identify vulnerabilities before deployment
- C) Encrypt all container data at rest
- D) Configure role-based access control for container administrators

94. **What is the main goal of using digital certificates in a public key infrastructure (PKI)?**
- A) Encrypt communications between devices
- B) Ensure the authenticity of a public key
- C) Generate secure passwords for users
- D) Monitor unauthorized access attempts

95. **An attacker uses a legitimate-looking website to trick users into entering sensitive information. What type of attack is this?**
- A) Spear phishing
- B) Watering hole attack
- C) Pharming
- D) Whaling

96. **During a forensic investigation, what is the first step to preserve evidence from a compromised system?**
- A) Isolate the system from the network
- B) Create a bit-by-bit image of the system
- C) Analyze logs for suspicious activity
- D) Restore the system from backup

97. **What is the primary purpose of using data loss prevention (DLP) tools?**
- A) Encrypt data stored in the cloud
- B) Prevent unauthorized transmission of sensitive data
- C) Detect malware in email attachments
- D) Monitor user activity on endpoints

98. **An organization discovers a vulnerable legacy system on its network that cannot be updated. What is the best mitigation strategy?**
- A) Implement micro-segmentation to isolate the system
- B) Encrypt all communications to and from the system
- C) Deploy endpoint detection and response (EDR) solutions
- D) Increase monitoring of system access logs

99. **Which control would best protect against a replay attack?**
- A) Multi-factor authentication
- B) Use of session tokens with timestamps
- C) End-to-end encryption

- D) Hashing sensitive data before storage

100. **An attacker exploits a misconfigured S3 bucket to access sensitive files. What is the best way to prevent such attacks in the future?**

- A) Use automated tools to check cloud configurations for vulnerabilities
- B) Encrypt all files stored in the S3 bucket
- C) Restrict public access to the S3 bucket
- D) Enable logging to monitor all file access events
