Satender Kumar - Final Exam: CompTIA Security+ (SY0-701)

1. **A company implements a Zero Trust model to secure its infrastructure. What is the core principle of this model?**
   - A) Implicit trust within the internal network
   - B) Continuous authentication and least privilege
   - C) Network segmentation with firewalls
   - D) Encrypting all data stored on-premises
2. **An attacker exploits a weak API endpoint to access sensitive customer data. What is the best defense against such attacks?**
   - A) Encrypt all API communications
   - B) Require multi-factor authentication for API users
   - C) Use input validation and rate limiting
   - D) Deploy endpoint protection on developer systems
3. **What is the primary purpose of a Business Impact Analysis (BIA)?**
   - A) Ensure compliance with regulatory frameworks
   - B) Identify critical business functions and assess the impact of disruptions
   - C) Detect insider threats through behavior monitoring
   - D) Analyze vulnerabilities in legacy systems
4. **A company experiences a ransomware attack. The attackers demand payment to decrypt critical files. What should the incident response team prioritize?**
   - A) Notify law enforcement and preserve evidence
   - B) Pay the ransom to restore operations quickly
   - C) Isolate affected systems and restore from backups
   - D) Disable all network traffic to contain the attack
5. **Which cryptographic technique ensures the integrity of a transmitted file?**
   - A) Encryption
   - B) Hashing
   - C) Tokenization
   - D) Salting
6. **An attacker sends phishing emails targeting executives of an organization. What is this attack called?**
   - A) Spear phishing
   - B) Whaling
   - C) Vishing
   - D) Smishing
7. **Which of the following is a primary function of a Security Information and Event Management (SIEM) system?**
   - A) Encrypt sensitive files in real-time
   - B) Analyze and correlate security events across the network
   - C) Automatically patch vulnerable systems
   - D) Deploy firewalls and intrusion prevention systems
8. **What is the best method to secure data stored in a misconfigured cloud storage bucket?**
   - A) Restrict public access and implement identity-based permissions
   - B) Encrypt all files with RSA
   - C) Configure logging to monitor access attempts
   - D) Deploy an intrusion detection system (IDS)
9. **An attacker intercepts and modifies communication between two devices. What is this attack called?**
   - A) Replay attack

- B) Man-in-the-middle (MITM)
- C) ARP poisoning
- D) Session hijacking

10. **Which of the following tools is used to analyze network traffic for suspicious activity?**
    - A) Wireshark
    - B) Nessus
    - C) Splunk
    - D) Metasploit
11. **What is the best defense against credential stuffing attacks?**
    - A) Enforce complex password policies
    - B) Deploy account lockout mechanisms and multi-factor authentication
    - C) Monitor network traffic for anomalies
    - D) Require password rotation every 90 days
12. **An organization notices a significant increase in outbound traffic to an unfamiliar IP address. What is the most likely explanation?**
    - A) Brute force attack
    - B) Data exfiltration via a compromised system
    - C) Network misconfiguration
    - D) Malware scanning the internal network
13. **Which of the following is a key feature of WPA3 for wireless networks?**
    - A) Secure Key Exchange (KRACK prevention)
    - B) Advanced Encryption Standard (AES)
    - C) Opportunistic Wireless Encryption (OWE)
    - D) Perfect Forward Secrecy
14. **What is the primary purpose of using a honeypot in a network?**
    - A) Divert attackers and gather intelligence
    - B) Encrypt sensitive data stored on the server
    - C) Prevent denial-of-service attacks
    - D) Detect and block phishing emails
15. **What is the best way to prevent SQL injection attacks?**
    - A) Use parameterized queries and input validation
    - B) Encrypt all sensitive database records
    - C) Deploy a web application firewall (WAF)
    - D) Implement multi-factor authentication
16. **An attacker exploits a buffer overflow vulnerability in an application. What is the likely goal?**
    - A) Gain administrative access to the server
    - B) Execute arbitrary code
    - C) Steal user credentials
    - D) Modify sensitive data
17. **Which regulatory framework governs the protection of payment card data?**
    - A) HIPAA
    - B) PCI DSS
    - C) GDPR
    - D) ISO 27001
18. **What is the primary purpose of network segmentation?**
    - A) Limit the spread of malware within the network
    - B) Encrypt sensitive communications
    - C) Improve network performance
    - D) Monitor all inbound and outbound traffic
19. **Which of the following controls is an example of a compensating control?**

    - A) Using a bastion host to access internal servers
    - B) Encrypting sensitive data in transit
    - C) Deploying a SIEM to correlate security events
    - D) Implementing multi-factor authentication for privileged accounts
20. **An attacker exploits a web application vulnerability to steal session tokens. What is the best way to mitigate this risk?**
    - A) Encrypt session tokens using HTTPS
    - B) Use input validation to sanitize user data
    - C) Implement secure cookie attributes and session timeouts
    - D) Deploy a firewall to block malicious traffic
21. **A network administrator discovers multiple failed login attempts on a critical server from different geographic locations. What is the most likely type of attack?**

- A) Credential stuffing
- B) Password spraying
- C) Brute force
- D) Replay attack

22. **What is the primary benefit of implementing network access control (NAC) in an organization?**

- A) Encrypt data in transit across the network
- B) Prevent unauthorized devices from connecting to the network
- C) Monitor user activity in real-time
- D) Ensure compliance with data privacy laws

23. **An attacker exploits an unpatched operating system to execute a remote code attack. What is the best remediation strategy?**

- A) Conduct real-time monitoring of system logs
- B) Enforce strict password policies
- C) Implement regular patch management processes
- D) Deploy endpoint detection and response (EDR) solutions

24. **What is the main purpose of a certificate revocation list (CRL) in PKI?**

- A) Provide encryption for sensitive communications
- B) Validate digital signatures
- C) Identify and revoke invalid or compromised certificates
- D) Authenticate public and private keys

25. **Which of the following attacks targets Bluetooth-enabled devices to gain unauthorized access?**

- A) Bluesnarfing
- B) Bluejacking
- C) Rogue AP
- D) Evil twin

26. **What is the best way to mitigate risks associated with shadow IT within an organization?**

- A) Block unapproved software installations on endpoints
- B) Conduct regular security awareness training
- C) Enforce a policy allowing only approved cloud services
- D) Monitor network traffic for unauthorized applications

27. **An attacker exploits a vulnerability in the database management system to retrieve customer data. What is the likely attack method?**

- A) SQL injection
- B) Command injection
- C) Cross-site scripting (XSS)
- D) Privilege escalation

28. **Which type of malware uses encryption to hold a victim's data hostage until a payment is made?**
- A) Spyware
- B) Rootkit
- C) Ransomware
- D) Worm

29. **A company wants to improve security on its wireless network. Which technology provides the strongest encryption and key management?**
- A) WEP
- B) WPA2
- C) WPA3
- D) TKIP

30. **An attacker modifies a web application's URL parameters to gain unauthorized access to resources. What is the best defense against this attack?**
- A) Encrypt all HTTP traffic using HTTPS
- B) Validate and sanitize user input at the server level
- C) Deploy a firewall between the application and the database
- D) Implement multi-factor authentication

31. **Which tool is best for analyzing packet-level traffic during a suspected network breach?**
- A) Wireshark
- B) Nessus
- C) Metasploit
- D) Splunk

32. **A malicious actor exploits a misconfigured S3 bucket to access sensitive files. What is the best remediation?**
- A) Enable logging to monitor access to the bucket
- B) Restrict public access to the bucket and implement access control policies
- C) Encrypt all files stored in the bucket
- D) Use endpoint protection on systems accessing the bucket

33. **An attacker exploits a man-in-the-middle vulnerability on an unsecured wireless network. What is the best way to mitigate this risk?**
- A) Enable WPA3 encryption
- B) Require VPN connections for wireless users
- C) Block access to public Wi-Fi networks
- D) Configure static IP addresses for all devices

34. **Which security principle is enforced by requiring users to authenticate with both a password and a hardware token?**
- A) Non-repudiation
- B) Multi-factor authentication
- C) Integrity
- D) Least privilege

35. **An organization uses a third-party vendor for cloud services. What is the best way to ensure compliance with security standards?**
- A) Encrypt all communications between the organization and the cloud provider
- B) Review and enforce the service-level agreement (SLA)
- C) Monitor the cloud environment with a SIEM solution
- D) Deploy endpoint detection on all cloud servers

36. **What is the main purpose of a data loss prevention (DLP) solution?**
- A) Prevent unauthorized transmission of sensitive data
- B) Monitor network traffic for malware
- C) Encrypt data in transit and at rest

- D) Detect and block phishing emails

37. **What is the most effective way to reduce the risk of insider threats?**
- A) Conduct regular background checks on employees
- B) Implement access controls and continuous monitoring
- C) Deploy endpoint detection and response (EDR) tools
- D) Require complex passwords for all users

38. **An attacker uses stolen credentials to gain access to a network. What is the most effective prevention mechanism?**
- A) Multi-factor authentication (MFA)
- B) Role-based access control (RBAC)
- C) Security awareness training
- D) Endpoint encryption

39. **Which protocol ensures that DNS responses are authentic and have not been tampered with?**
- A) DNSSEC
- B) TLS
- C) HTTPS
- D) S/MIME

40. **What is the primary advantage of using elliptic curve cryptography (ECC) over RSA?**
- A) Faster key generation and encryption with shorter key lengths
- B) Supports hashing for data integrity
- C) Offers greater resistance to brute-force attacks
- D) Provides easier certificate management

41. **What is the primary purpose of implementing multi-factor authentication (MFA) for privileged accounts?**
- A) Increase password complexity requirements
- B) Reduce the risk of unauthorized access
- C) Encrypt all privileged account communications
- D) Monitor all login attempts in real-time

42. **Which tool would best identify security vulnerabilities in a web application before deployment?**
- A) Static Application Security Testing (SAST)
- B) Intrusion Prevention System (IPS)
- C) Endpoint Detection and Response (EDR)
- D) Packet analyzer

43. **An organization implements a honeynet in its infrastructure. What is the primary purpose of this strategy?**
- A) Prevent malware infections on critical systems
- B) Divert attackers and gather intelligence about their methods
- C) Encrypt sensitive data on the network
- D) Test new security patches in a controlled environment

44. **What is the best way to mitigate risks associated with an unsecured IoT device connected to a corporate network?**
- A) Use endpoint protection on the device
- B) Implement network segmentation for IoT devices
- C) Deploy a firewall to monitor device activity
- D) Encrypt all communications to and from the device

45. **An attacker exploits a vulnerability in a web application by injecting malicious JavaScript into input fields. What is this type of attack called?**
- A) SQL injection
- B) Cross-site scripting (XSS)

- C) Command injection
- D) Directory traversal

46. **Which security control ensures that log files cannot be tampered with after they are created?**
- A) Encrypt logs before storing them
- B) Store logs on write-once-read-many (WORM) media
- C) Rotate log files every 24 hours
- D) Monitor logs with a SIEM system

47. **A security analyst identifies outbound traffic to a known malicious IP address. What should be the first action?**
- A) Isolate the affected system from the network
- B) Notify the incident response team
- C) Block the IP address at the firewall
- D) Conduct a vulnerability scan on the affected system

48. **Which of the following best prevents replay attacks on a network?**
- A) Use encrypted session tokens with timestamps
- B) Implement role-based access control
- C) Require multi-factor authentication for all users
- D) Deploy a web application firewall (WAF)

49. **What is the purpose of using Perfect Forward Secrecy (PFS) in cryptographic communications?**
- A) Ensure that session keys are not reused
- B) Protect against phishing attacks
- C) Simplify key management for large-scale systems
- D) Authenticate endpoints before communication

50. **Which technology best protects a cloud storage bucket from unauthorized access?**
- A) Enable encryption for all stored data
- B) Restrict bucket access using identity-based permissions
- C) Configure static IP addresses for all accessing devices
- D) Monitor bucket access logs with a SIEM solution

51. **A security analyst observes high CPU usage on a server, and traffic analysis reveals outbound requests to random IP addresses. What is the most likely cause?**
- A) Botnet activity
- B) SQL injection attack
- C) Insider threat
- D) Brute force attack

52. **What is the primary function of Transport Layer Security (TLS) in securing web applications?**
- A) Prevent unauthorized access to the application's code
- B) Encrypt data in transit to ensure confidentiality and integrity
- C) Block malicious HTTP requests to the application
- D) Authenticate application users

53. **An attacker gains unauthorized access to an account by using credentials leaked in a data breach. What is the best mitigation strategy?**
- A) Monitor access logs for anomalies
- B) Implement multi-factor authentication (MFA)
- C) Encrypt stored credentials with AES
- D) Require password changes every 90 days

54. **Which of the following mitigates the risk of insider threats?**
- A) Conduct background checks and enforce least privilege access policies
- B) Implement a honeynet to detect malicious activity

- C) Encrypt all internal communications
- D) Deploy intrusion detection systems (IDS)

55. **Which regulatory framework is designed to protect the privacy and security of healthcare information?**
- A) PCI DSS
- B) GDPR
- C) HIPAA
- D) ISO 27001

56. **An organization uses a Security Orchestration, Automation, and Response (SOAR) platform. What is the main benefit of this tool?**
- A) Automatically block all malicious traffic
- B) Correlate logs from multiple sources for real-time alerts
- C) Automate incident response workflows and reduce manual effort
- D) Encrypt sensitive data in cloud environments

57. **An attacker gains access to sensitive files by exploiting an improperly configured directory. What is this type of attack called?**
- A) Command injection
- B) Directory traversal
- C) Buffer overflow
- D) Privilege escalation

58. **What is the primary advantage of using elliptic curve cryptography (ECC) over traditional RSA encryption?**
- A) Faster encryption and shorter key lengths with equivalent security
- B) Simplified key management processes
- C) Greater resistance to phishing attacks
- D) Increased scalability for large networks

59. **An attacker sends an email containing a malicious link that appears to be from a trusted source. What is this type of attack called?**
- A) Whaling
- B) Smishing
- C) Phishing
- D) Spear phishing

60. **What is the primary purpose of a vulnerability scan in a security program?**
- A) Block malicious network traffic
- B) Identify and prioritize weaknesses in systems and applications
- C) Monitor user activity across the network
- D) Test the effectiveness of incident response plans

61. **Which of the following is the most effective way to prevent brute force attacks on a remote login portal?**
- A) Use CAPTCHA after a number of failed attempts
- B) Encrypt all login attempts using AES
- C) Require password rotation every 60 days
- D) Implement account lockout and multi-factor authentication

62. **An attacker exploits a web application vulnerability that allows unauthorized access to a backend database. What type of attack is this?**
- A) SQL injection
- B) Cross-site scripting (XSS)
- C) Directory traversal
- D) Session hijacking

63. **What is the main purpose of role-based access control (RBAC)?**
- A) Limit user permissions to their specific job responsibilities

- B) Encrypt sensitive files at rest
- C) Monitor user activity on critical systems
- D) Provide multi-factor authentication for privileged accounts

64. **An organization uses security labels to enforce access control policies based on data classification. Which access control model does this represent?**
- A) Discretionary Access Control (DAC)
- B) Mandatory Access Control (MAC)
- C) Attribute-Based Access Control (ABAC)
- D) Role-Based Access Control (RBAC)

65. **A penetration tester successfully exploits an unpatched vulnerability in a network service. What should the tester do next?**
- A) Immediately escalate privileges on the target system
- B) Notify the organization and document the vulnerability
- C) Conduct further testing to identify additional weaknesses
- D) Disconnect the system to prevent further exploitation

66. **Which of the following tools is best for identifying vulnerabilities in a running network environment?**
- A) Nessus
- B) Wireshark
- C) Splunk
- D) Metasploit

67. **What is the primary function of a demilitarized zone (DMZ) in a network architecture?**
- A) Encrypt sensitive traffic between internal and external systems
- B) Host public-facing services and isolate them from the internal network
- C) Monitor and log all network traffic
- D) Detect and block malicious traffic before it reaches the network

68. **An organization implements a data loss prevention (DLP) solution. What is its primary purpose?**
- A) Detect and block unauthorized access to critical systems
- B) Prevent sensitive data from leaving the organization
- C) Encrypt data in transit and at rest
- D) Monitor employee activity across the network

69. **Which attack involves redirecting legitimate traffic to a malicious website by altering DNS entries?**
- A) Man-in-the-middle (MITM)
- B) DNS poisoning
- C) ARP spoofing
- D) Evil twin attack

70. **What is the primary purpose of salting in password security?**
- A) Encrypt passwords in storage
- B) Prevent brute force and rainbow table attacks
- C) Ensure backward compatibility with older authentication systems
- D) Simplify password management for users

71. **A security analyst notices an increase in outbound traffic from an IoT device. What is the most likely explanation?**
- A) The device is scanning the network for vulnerabilities
- B) The device is part of a botnet performing a DDoS attack
- C) The device has been infected with ransomware
- D) The device is sending updates to its vendor

72. **Which of the following ensures that sensitive data is not altered during transmission?**
- A) Hashing

- B) Encryption
- C) Tokenization
- D) Salting

73. **An attacker uses stolen session tokens to impersonate a legitimate user. What is the best mitigation for this risk?**
- A) Implement secure cookie attributes and session timeouts
- B) Encrypt all communications using TLS
- C) Deploy a web application firewall (WAF)
- D) Use multi-factor authentication

74. **What is the primary benefit of network segmentation in cybersecurity?**
- A) Prevent unauthorized devices from connecting to the network
- B) Limit the spread of malware and unauthorized access within the network
- C) Encrypt traffic between all devices on the network
- D) Simplify network monitoring and performance tuning

75. **Which attack involves using a fraudulent wireless access point to intercept sensitive information?**
- A) Evil twin attack
- B) Bluejacking
- C) Rogue AP
- D) ARP poisoning

76. **An attacker sends phishing emails to a specific group within an organization. What is this type of attack called?**
- A) Whaling
- B) Spear phishing
- C) Vishing
- D) Smishing

77. **An organization wants to enforce time-based restrictions for user access to its systems. What is the best approach?**
- A) Implement time-based access control policies
- B) Use role-based access control (RBAC)
- C) Deploy a web application firewall (WAF)
- D) Encrypt user credentials

78. **What is the main function of a vulnerability scanner?**
- A) Identify security gaps in systems and applications
- B) Block unauthorized access attempts
- C) Encrypt sensitive data during transmission
- D) Monitor user behavior on the network

79. **An attacker exploits a Bluetooth vulnerability to access data on a mobile device. What type of attack is this?**
- A) Bluejacking
- B) Bluesnarfing
- C) Evil twin attack
- D) Rogue AP

80. **An organization uses a certificate revocation list (CRL) as part of its public key infrastructure (PKI). What is the purpose of this list?**
- A) Provide encryption for sensitive data
- B) Track and revoke compromised digital certificates
- C) Validate public and private key pairs
- D) Authenticate the identity of certificate holders

81. **Which technology best prevents unauthorized access to network resources by evaluating the health of devices before granting access?**

- A) Network Access Control (NAC)
- B) Endpoint Detection and Response (EDR)
- C) Intrusion Prevention System (IPS)
- D) Security Information and Event Management (SIEM)

82. **An attacker uses a compromised account to access an organization's email system and send phishing emails to internal employees. What type of attack is this?**
- A) Whaling
- B) Business Email Compromise (BEC)
- C) Phishing
- D) Spear phishing

83. **What is the best way to mitigate risks associated with unpatched vulnerabilities in an operating system?**
- A) Use intrusion prevention systems (IPS)
- B) Implement a robust patch management process
- C) Require multi-factor authentication for all users
- D) Encrypt all traffic to and from the affected system

84. **Which of the following best ensures the confidentiality of data in a cloud storage bucket?**
- A) Encrypt data at rest and in transit
- B) Use a web application firewall (WAF)
- C) Deploy endpoint protection on client systems
- D) Implement tokenization for sensitive data

85. **An organization experiences a Distributed Denial of Service (DDoS) attack targeting its public website. What is the best immediate action?**
- A) Block traffic from suspicious IP addresses using a firewall
- B) Notify users of service downtime
- C) Deploy a cloud-based DDoS mitigation service
- D) Increase server capacity to handle the traffic

86. **What is the primary purpose of implementing Perfect Forward Secrecy (PFS) in encryption protocols?**
- A) Prevent the reuse of session keys
- B) Strengthen hashing algorithms for data integrity
- C) Simplify key rotation policies
- D) Detect unauthorized modifications to encrypted data

87. **Which tool is commonly used to simulate attacks and test the security posture of a system?**
- A) Metasploit
- B) Nessus
- C) Wireshark
- D) Splunk

88. **What is the best way to prevent unauthorized devices from connecting to a corporate wireless network?**
- A) Enable WPA3 encryption
- B) Deploy a Network Access Control (NAC) solution
- C) Use endpoint detection tools
- D) Implement static IP addressing

89. **An organization wants to ensure that sensitive email communications cannot be read by unauthorized parties. Which protocol should it use?**
- A) S/MIME
- B) TLS
- C) SSH
- D) IPsec

90. **An attacker sends specially crafted packets to exploit a buffer overflow vulnerability in a web server. What is the likely goal?**
- A) Steal sensitive data from the server
- B) Execute arbitrary code on the server
- C) Redirect traffic to a malicious website
- D) Crash the server to cause downtime

91. **Which practice minimizes the attack surface of an application by reducing unnecessary features and components?**
- A) Hardening
- B) Tokenization
- C) Network segmentation
- D) Input validation

92. **An attacker exploits a weak password policy to gain unauthorized access to an administrator account. What is the best remediation?**
- A) Implement password complexity requirements
- B) Encrypt all stored passwords with AES
- C) Require regular password changes
- D) Use biometric authentication for administrator accounts

93. **What is the primary function of Transport Layer Security (TLS) in web applications?**
- A) Provide end-to-end encryption for data in transit
- B) Block unauthorized traffic to the application
- C) Authenticate the application server
- D) Detect and log malicious activity

94. **An attacker manipulates DNS cache entries to redirect users to malicious websites. What is this attack called?**
- A) DNS poisoning
- B) ARP spoofing
- C) Evil twin
- D) Replay attack

95. **Which type of malware is designed to operate stealthily at the kernel level, granting attackers persistent access?**
- A) Rootkit
- B) Trojan
- C) Worm
- D) Spyware

96. **What is the primary advantage of elliptic curve cryptography (ECC) over traditional cryptographic algorithms like RSA?**
- A) Shorter key lengths with equivalent security strength
- B) Enhanced resistance to quantum attacks
- C) Simplified certificate management
- D) Greater compatibility with legacy systems

97. **What is the purpose of a Security Orchestration, Automation, and Response (SOAR) platform?**
- A) Encrypt sensitive communications
- B) Automate incident response workflows and improve efficiency
- C) Block phishing emails and detect malware
- D) Provide vulnerability scanning for endpoints

98. **An organization implements context-aware access control. What does this approach enable?**
- A) Limit access based on user behavior, location, and device type
- B) Allow access only during predefined time windows

- C) Restrict access based on user roles and responsibilities
- D) Encrypt all data transmissions between devices

99. **Which regulatory framework focuses on securing financial records and ensuring accountability in public companies?**

- A) GDPR
- B) PCI DSS
- C) HIPAA
- D) Sarbanes-Oxley Act (SOX)

100. **What is the best way to mitigate risks associated with credential stuffing attacks?**

- A) Deploy multi-factor authentication (MFA)
- B) Encrypt stored passwords using SHA-256
- C) Require password changes every 90 days
- D) Block repeated login attempts from the same IP address