Satender KumarPractice Test 3 - CompTIA Security+ (SY0-701).

1. **An employee receives an email with an attachment that appears to be an invoice from a known vendor. When the attachment is opened, ransomware encrypts the user's files. What is the best prevention method for this scenario?**
   - ○ A) Regular vulnerability scanning
   - ○ B) User training on recognizing phishing emails
   - ○ C) Deployment of an intrusion prevention system (IPS)
   - ○ D) Blocking all email attachments
2. **Which type of firewall inspects the content of packets at the application layer to detect and block threats?**
   - ○ A) Stateful firewall
   - ○ B) Packet-filtering firewall
   - ○ C) Next-generation firewall (NGFW)
   - ○ D) Circuit-level gateway
3. **What is the primary purpose of Security Information and Event Management (SIEM) solutions?**
   - ○ A) Encrypt sensitive data in transit
   - ○ B) Correlate and analyze security logs in real-time
   - ○ C) Prevent malware infections on endpoints
   - ○ D) Automate vulnerability management
4. **An attacker gains access to a user's online banking account by guessing their weak password. What is the most effective mitigation for this attack?**
   - ○ A) Use password complexity policies
   - ○ B) Implement multi-factor authentication (MFA)
   - ○ C) Deploy a web application firewall (WAF)
   - ○ D) Require password changes every 30 days
5. **A security team identifies a rogue device connected to the corporate network. What is the best action to take?**
   - ○ A) Block the device's MAC address on the network
   - ○ B) Isolate the device using network segmentation
   - ○ C) Deploy an endpoint detection and response (EDR) solution
   - ○ D) Shut down the network switch to prevent further connections
6. **Which cryptographic method is used to ensure the authenticity of software updates?**
   - ○ A) Symmetric encryption
   - ○ B) Digital signatures
   - ○ C) Hashing with MD5
   - ○ D) Elliptic curve cryptography (ECC)
7. **A company experiences a DDoS attack targeting its e-commerce platform. What is the best immediate action?**
   - ○ A) Deploy a load balancer to distribute traffic
   - ○ B) Block all incoming traffic on the affected port
   - ○ C) Redirect traffic through a cloud-based DDoS mitigation service
   - ○ D) Notify customers of service downtime
8. **What is the primary purpose of using a honeypot in a network?**
   - ○ A) Divert attackers and gather intelligence about their methods
   - ○ B) Encrypt sensitive data stored in the database
   - ○ C) Prevent brute-force attacks on user accounts
   - ○ D) Analyze legitimate user behavior
9. **Which protocol ensures the confidentiality and integrity of email communications?**

- A) S/MIME
- B) SMTP
- C) IMAP
- D) POP3

10. **An attacker uses a script to repeatedly try default usernames and passwords on IoT devices. What type of attack is this?**
    - A) Brute force
    - B) Credential stuffing
    - C) Password spraying
    - D) Dictionary attack
11. **Which type of control is a physical lock used to secure server racks?**
    - A) Detective
    - B) Preventive
    - C) Corrective
    - D) Compensating
12. **An attacker modifies ARP cache entries on a target system to intercept network traffic. What is this attack called?**
    - A) DNS poisoning
    - B) Man-in-the-middle (MITM)
    - C) ARP spoofing
    - D) Packet injection
13. **What is the primary purpose of a Business Continuity Plan (BCP)?**
    - A) Detect and mitigate malware infections
    - B) Ensure the availability of critical business operations during disruptions
    - C) Identify gaps in organizational security
    - D) Provide training for incident response teams
14. **An organization deploys a proxy server to block access to malicious websites. What type of control does this represent?**
    - A) Preventive
    - B) Corrective
    - C) Detective
    - D) Compensating
15. **An attacker injects malicious SQL statements into a web application's input field. What is the best defense against this attack?**
    - A) Input validation and parameterized queries
    - B) Encrypt all database records
    - C) Implement multi-factor authentication
    - D) Deploy a network intrusion detection system
16. **Which practice helps reduce the risk of insider threats?**
    - A) Conduct regular security awareness training
    - B) Implement a host-based firewall
    - C) Use a web application firewall (WAF)
    - D) Encrypt sensitive data at rest
17. **What is the purpose of perfect forward secrecy (PFS) in encryption?**
    - A) Protect against session key compromise
    - B) Provide faster encryption and decryption
    - C) Encrypt data using symmetric keys
    - D) Prevent brute-force attacks
18. **Which type of vulnerability allows attackers to execute arbitrary code by exploiting an application’s memory handling?**
    - A) Buffer overflow

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

19. **What is the best way to mitigate the risks associated with shadow IT in an organization?**
    - A) Deploy endpoint protection on all devices
    - B) Implement strict access control policies
    - C) Educate employees about approved tools and services
    - D) Encrypt all sensitive data
20. **Which type of malware remains hidden within a system and provides unauthorized access to an attacker?**
    - A) Trojan
    - B) Rootkit
    - C) Spyware
    - D) Logic bomb
21. **What is the primary function of Transport Layer Security (TLS)?**
    - A) Encrypt web traffic to ensure confidentiality and integrity
    - B) Authenticate users to web applications
    - C) Detect unauthorized modifications to files
    - D) Block unauthorized network connections
22. **A security analyst identifies that attackers are using brute force methods to guess admin passwords. What is the best mitigation strategy?**
    - A) Implement account lockout policies
    - B) Require password rotation every 30 days
    - C) Deploy a firewall to block incoming connections
    - D) Use a SIEM solution for monitoring
23. **An organization wants to ensure that only authorized users can access its sensitive data. What type of encryption should be used?**
    - A) Symmetric encryption
    - B) Asymmetric encryption
    - C) Hashing
    - D) Tokenization
24. **An attacker exploits a software vulnerability to gain administrative privileges on a system. What type of attack is this?**
    - A) Privilege escalation
    - B) Credential stuffing
    - C) Social engineering
    - D) Denial-of-service
25. **A user reports that their system is infected with ransomware. What is the first action the incident response team should take?**
    - A) Isolate the infected system from the network
    - B) Decrypt the files using a backup key
    - C) Analyze the attack using a SIEM solution
    - D) Notify law enforcement
26. **An attacker uses email spoofing to impersonate a senior executive and requests a wire transfer from the finance department. What type of attack is this?**

- A) Whaling
- B) Vishing
- C) Credential stuffing
- D) Pretexting

27. **Which of the following controls is most effective in preventing unauthorized physical access to a secure data center?**

- A) Role-based access control
- B) Biometric authentication
- C) Security awareness training
- D) Two-factor authentication

28. **What is the primary purpose of a vulnerability scanner?**

- A) Detect malware on endpoints
- B) Identify security gaps in systems and applications
- C) Block unauthorized network traffic
- D) Encrypt sensitive data during transmission

29. **Which type of malware allows attackers to gain persistent, unauthorized access to a system by exploiting system-level privileges?**

- A) Ransomware
- B) Rootkit
- C) Worm
- D) Keylogger

30. **What is the best way to secure backups stored in an offsite location?**

- A) Use hashing to verify the integrity of backup files
- B) Encrypt backups with strong encryption algorithms
- C) Limit physical access to the backup facility
- D) Replicate backups to multiple locations

31. **An organization wants to protect its network from DDoS attacks. What is the best solution?**

- A) Implement a content delivery network (CDN) with DDoS mitigation capabilities
- B) Deploy endpoint detection and response (EDR) tools
- C) Configure access control lists (ACLs) on network devices
- D) Use a virtual private network (VPN) for all connections

32. **Which of the following tools is used to analyze packet-level traffic on a network?**

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

33. **What is the primary purpose of a Security Orchestration, Automation, and Response (SOAR) platform?**

- A) Automate incident response workflows
- B) Prevent phishing emails from reaching users
- C) Provide endpoint protection against malware
- D) Enforce zero-trust policies across the organization

34. **Which type of attack involves embedding malicious scripts in trusted websites to execute on a victim's browser?**

- A) SQL injection
- B) Cross-site scripting (XSS)
- C) Watering hole attack
- D) Command injection

35. **An attacker exploits a weak API endpoint to gain unauthorized access to a database. What is the best way to prevent such attacks?**

- A) Use input validation and access control measures
- B) Encrypt all API communications
- C) Deploy a web application firewall (WAF)
- D) Require multi-factor authentication for API users

36. **What is the main advantage of using asymmetric encryption for secure communications?**

- A) It uses the same key for encryption and decryption
- B) It enables secure key exchange over an insecure channel

- C) It encrypts data faster than symmetric encryption
- D) It provides integrity checks for transmitted data

37. **Which technique is most effective for preventing privilege escalation attacks?**

- A) Regularly update system patches
- B) Implement role-based access control (RBAC)
- C) Conduct penetration testing on critical applications
- D) Deploy a Security Information and Event Management (SIEM) system

38. **Which attack targets Bluetooth-enabled devices to gain unauthorized access?**

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

39. **A company wants to ensure its employees access sensitive resources only during work hours. What is the best solution?**

- A) Implement time-based access control policies
- B) Deploy a network intrusion prevention system
- C) Enforce multi-factor authentication
- D) Use endpoint encryption

40. **What is the purpose of using a data loss prevention (DLP) solution?**

- A) Detect and block attempts to exfiltrate sensitive data
- B) Encrypt data stored on servers
- C) Prevent malware from infecting endpoints
- D) Monitor user behavior for anomalies

41. **An attacker successfully performs a DNS cache poisoning attack. What is the likely outcome?**

- A) Users are redirected to malicious websites when accessing legitimate domains
- B) Network traffic is encrypted by the attacker
- C) Unauthorized users gain access to internal systems
- D) Sensitive data is exfiltrated to external servers

42. **What is the best method to ensure a cloud storage bucket is secure?**

- A) Enable encryption for all stored files
- B) Implement public-read permissions for select users
- C) Use automated tools to scan for misconfigurations
- D) Restrict access to authenticated users only

43. **What is the primary purpose of a demilitarized zone (DMZ) in a network?**

- A) Encrypt all traffic between devices
- B) Isolate public-facing services from the internal network
- C) Monitor and log internal network activity
- D) Prevent malware from spreading

44. **Which type of attack leverages stolen session tokens to impersonate a user?**

- A) Replay attack
- B) Cross-site request forgery (CSRF)
- C) Session hijacking
- D) Credential stuffing

45. **A company experiences a phishing campaign targeting its employees. What is the best mitigation step?**

- A) Enable email filtering with spam detection
- B) Require users to change passwords weekly
- C) Implement endpoint detection and response (EDR) solutions
- D) Block all external emails temporarily

46. **What is the best way to mitigate the risk of data exfiltration via USB devices?**

- A) Disable USB ports on all corporate devices
- B) Deploy endpoint data loss prevention (DLP) tools
- C) Encrypt all removable drives used within the organization
- D) Conduct regular vulnerability scans

47. **An attacker sends malicious code to a web application that executes in the browser of other users. What is the type of attack?**

- A) SQL injection
- B) Cross-site scripting (XSS)
- C) Buffer overflow
- D) Watering hole attack

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

- A) Store public and private keys securely
- B) Verify the authenticity of certificates
- C) List certificates that are no longer valid
- D) Encrypt sensitive data in transit

49. **Which of the following ensures that unauthorized changes to critical system files are detected?**

- A) File integrity monitoring (FIM)
- B) Intrusion prevention system (IPS)
- C) Host-based firewall
- D) Static application security testing (SAST)

50. **An organization wants to prioritize risk mitigation efforts. Which metric should be considered first?**

- A) Annualized Loss Expectancy (ALE)
- B) Recovery Time Objective (RTO)
- C) Mean Time Between Failures (MTBF)
- D) Maximum Tolerable Downtime (MTD)

51. **An attacker intercepts communications between two devices and modifies the transmitted data. What type of attack is this?**

- A) Man-in-the-middle
- B) DNS poisoning
- C) Replay attack
- D) Packet sniffing

52. **What is the most effective way to protect data stored in a cloud environment?**

- A) Encrypt data at rest and in transit
- B) Configure a web application firewall (WAF)
- C) Deploy an intrusion detection system (IDS)
- D) Use multi-factor authentication for access

53. **A security analyst observes that users are being redirected to malicious websites despite entering the correct URLs. What is the likely cause?**

- A) DNS spoofing
- B) SQL injection
- C) Evil twin attack
- D) ARP poisoning

54. **What is the primary function of a sandbox in malware analysis?**

- A) Isolate and observe malicious behavior in a controlled environment
- B) Encrypt files affected by malware
- C) Prevent malware from spreading within a network
- D) Patch vulnerabilities in compromised systems

55. **Which technique ensures that passwords stored in a database are resistant to brute force and rainbow table attacks?**

- A) Salting before hashing
- B) Encrypting passwords with AES
- C) Storing passwords in plaintext
- D) Using tokenization

56. **What is the purpose of using split tunneling in a VPN setup?**

- A) Encrypt all traffic over the VPN connection
- B) Route only specific traffic through the VPN
- C) Provide faster internet speeds for remote users
- D) Prevent unauthorized access to the VPN

57. **Which of the following ensures secure communication over an untrusted network?**

- A) Transport Layer Security (TLS)
- B) Simple Network Management Protocol (SNMP)
- C) Dynamic Host Configuration Protocol (DHCP)
- D) Domain Name System Security Extensions (DNSSEC)

58. **An attacker sends a phishing email to a specific group within an organization. What type of attack is this?**

- A) Spear phishing
- B) Whaling
- C) Vishing
- D) Smishing

59. **What is the primary benefit of a vulnerability management program?**

- A) Prevent malware infections on endpoints
- B) Identify and remediate security weaknesses
- C) Block unauthorized access to systems
- D) Provide continuous monitoring of network traffic

60. **An organization deploys biometric authentication to secure access to sensitive systems. What is the primary advantage of this method?**

- A) Resistance to phishing attacks
- B) Scalability across large networks
- C) Faster authentication processes
- D) High level of accuracy in user verification

61. **Which attack exploits a vulnerability in wireless encryption protocols to gain unauthorized access?**

- A) Evil twin attack
- B) Bluejacking
- C) KRACK (Key Reinstallation Attack)
- D) Rogue AP

62. **What is the main purpose of a risk register in cybersecurity?**

- A) Identify and track vulnerabilities in the network
- B) Document and prioritize identified risks
- C) Provide a checklist for compliance audits
- D) Track incident response metrics

63. **Which practice reduces the risk of phishing attacks?**

- A) Deploy endpoint detection and response (EDR) tools
- B) Implement email filtering with domain-based authentication (DMARC)
- C) Enforce complex password policies
- D) Use role-based access control (RBAC)

64. **What is the most effective way to defend against SQL injection attacks?**

- A) Encrypt database queries
- B) Use parameterized statements and input validation
- C) Implement a firewall between the application and database

- D) Enable logging on all database operations

65. **An organization wants to ensure the integrity of its sensitive files during transfer. Which cryptographic technique should it use?**

- A) Digital signatures
- B) Asymmetric encryption
- C) Symmetric encryption
- D) Hashing

66. **What type of malware locks a user's files and demands payment to unlock them?**

- A) Rootkit
- B) Ransomware
- C) Adware
- D) Worm

67. **Which of the following technologies best prevents data exfiltration from USB devices?**

- A) Endpoint Data Loss Prevention (DLP)
- B) Network Access Control (NAC)
- C) Intrusion Prevention System (IPS)
- D) File Integrity Monitoring (FIM)

68. **An attacker intercepts and resends legitimate communication to gain unauthorized access. What type of attack is this?**

- A) Replay attack
- B) Session hijacking
- C) Cross-site scripting (XSS)
- D) ARP spoofing

69. **What is the purpose of using Transport Layer Security (TLS) in web communications?**

- A) Encrypt data in transit to ensure confidentiality
- B) Authenticate users to web servers
- C) Detect unauthorized modifications to web pages
- D) Block malicious traffic from reaching endpoints

70. **An organization wants to restrict administrative access to its network devices. What is the best practice to implement?**

- A) Use a dedicated management VLAN
- B) Configure default usernames and passwords
- C) Allow remote access from any IP address
- D) Deploy host-based firewalls

71. **What is the primary purpose of using role-based access control (RBAC)?**

- A) Enforce least privilege for users
- B) Encrypt sensitive files on endpoints
- C) Monitor and log user activities
- D) Enable faster authentication

72. **Which security principle ensures that data is accessible to authorized users when needed?**

- A) Integrity
- B) Confidentiality
- C) Availability
- D) Non-repudiation

73. **Which attack involves tricking a victim into installing malware by mimicking a legitimate application update?**

- A) Drive-by download
- B) Trojan horse
- C) Phishing
- D) Rogue software

74. **What is the purpose of network segmentation in cybersecurity?**

- A) Limit the spread of malware within the network
- B) Encrypt sensitive traffic between devices
- C) Monitor and log all inbound traffic
- D) Detect unauthorized access attempts

75. **What is the best way to mitigate risks associated with legacy systems that cannot be updated?**

- A) Implement network segmentation to isolate legacy systems
- B) Deploy an intrusion prevention system (IPS)
- C) Require multi-factor authentication for all users
- D) Monitor user behavior with UEBA solutions

76. **Which security measure best prevents brute-force attacks on a login portal?**

- A) Require CAPTCHA for failed login attempts
- B) Enforce account lockout after several failed attempts
- C) Encrypt all login credentials using AES
- D) Require password changes every 30 days

77. **An attacker exploits a web application's vulnerability to execute commands on the server. What is this attack called?**

- A) SQL injection
- B) Cross-site scripting (XSS)
- C) Command injection
- D) Directory traversal

78. **Which of the following ensures secure communication between remote offices over the internet?**

- A) VLAN
- B) VPN
- C) IDS
- D) SIEM

79. **A security team detects unauthorized access to a privileged account after a phishing attack. What is the next step in the incident response process?**

- A) Notify affected users
- B) Disable the compromised account
- C) Review logs for further anomalies
- D) Conduct a forensic investigation

80. **Which cryptographic algorithm is used in WPA3 to secure wireless networks?**

- A) RSA
- B) AES
- C) ECC
- D) SHA-256

81. **What is the primary function of a file integrity monitoring (FIM) solution?**

- A) Prevent unauthorized file access
- B) Detect and alert on changes to critical files
- C) Encrypt files stored on endpoints
- D) Monitor and log user activity

82. **An organization deploys role-based access control (RBAC) for its HR systems. Which principle does this configuration enforce?**

- A) Confidentiality
- B) Least privilege
- C) Availability
- D) Non-repudiation

83. **What type of attack involves sending a fraudulent URL designed to steal login credentials?**

- A) Pharming

- B) Whaling
- C) Phishing
- D) Vishing

84. **Which vulnerability allows attackers to take control of an application by exploiting its memory management?**

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

85. **What is the purpose of a federated identity management system?**

- A) Provide multi-factor authentication for user accounts
- B) Allow single sign-on across multiple organizations
- C) Encrypt sensitive data during transmission
- D) Authenticate API endpoints securely

86. **Which tool would you use to analyze suspicious network traffic in real time?**

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

87. **An organization wants to prevent data exfiltration through removable media. What is the best solution?**

- A) Endpoint Data Loss Prevention (DLP)
- B) Multi-factor authentication
- C) Encrypt USB devices
- D) Role-based access control

88. **Which attack involves exploiting a browser vulnerability to execute arbitrary code on a victim's system?**

- A) Drive-by download
- B) Logic bomb
- C) ARP spoofing
- D) DNS poisoning

89. **What is the primary purpose of using salting in password hashing?**

- A) Increase computational complexity for attackers
- B) Encrypt passwords stored in a database
- C) Generate session keys dynamically
- D) Enable single sign-on for multiple systems

90. **A penetration tester successfully exploits an insecure API. What is the most effective remediation?**

- A) Implement input validation on API endpoints
- B) Encrypt all data transmitted through the API
- C) Require multi-factor authentication for all API users
- D) Deploy a SIEM to monitor API traffic

91. **What is the primary purpose of using network segmentation?**

- A) Enhance network performance by reducing traffic
- B) Limit the impact of a security breach
- C) Encrypt all traffic between network segments
- D) Simplify network device management

92. **Which type of malware operates at the kernel level to remain hidden and grant attackers unauthorized access?**

- A) Trojan
- B) Rootkit

- C) Spyware
- D) Worm

93. **What is the best practice for securing API endpoints exposed to the internet?**

- A) Use rate limiting to prevent abuse
- B) Implement role-based access control (RBAC)
- C) Enforce TLS for all API communications
- D) Use prepared statements for all inputs

94. **An attacker exploits a vulnerability to send multiple requests to a target web server, causing it to crash. What type of attack is this?**

- A) SQL injection
- B) Denial-of-service (DoS)
- C) Cross-site request forgery (CSRF)
- D) ARP poisoning

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

- A) Store private keys securely
- B) Validate the integrity of certificates
- C) Identify certificates that are no longer valid
- D) Encrypt communications between endpoints

96. **What is the best method to prevent unauthorized devices from accessing a corporate wireless network?**

- A) Deploy Network Access Control (NAC)
- B) Enable WPA3 encryption
- C) Require users to change passwords frequently
- D) Use endpoint detection and response (EDR)

97. **Which action ensures that data is not altered during transmission?**

- A) Encrypting data with AES
- B) Using hashing algorithms like SHA-256
- C) Implementing multi-factor authentication
- D) Deploying intrusion detection systems

98. **Which regulatory framework focuses on protecting healthcare information in the United States?**

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

99. **What is the best strategy to minimize the risk of insider threats?**

- A) Conduct regular security awareness training
- B) Encrypt sensitive data in transit and at rest
- C) Deploy endpoint detection and response (EDR) solutions
- D) Enforce strong password policies

100. **An attacker injects malicious scripts into a trusted website that executes in a user's browser. What is the best mitigation?**

- A) Validate all user input on the server side
- B) Encrypt all data stored in the database
- C) Block traffic from untrusted IPs
- D) Deploy endpoint protection software