100 MULTIPLE-CHOICE QUESTIONS TO PREPARE YOU FOR A CYBERSECURITY ANALYST INTERVIEW

BY IZZMIER IZZUDDIN

General Knowledge

1. What does CIA stand for in cybersecurity?
   a) Confidentiality, Integrity, Availability
   b) Cybersecurity, Integrity, Authentication
   c) Confidentiality, Integrity, Authentication
   d) Cybersecurity, Integrity, Availability

2. Which of the following is NOT a type of malware?
   a) Ransomware
   b) Spyware
   c) Firewall
   d) Trojan

3. What is the primary purpose of a firewall?
   a) Encrypt data
   b) Monitor network traffic and block unauthorised access
   c) Detect phishing emails
   d) Scan for viruses

4. Which protocol is used for secure communication over a computer network?
   a) HTTP
   b) FTP
   c) HTTPS
   d) SMTP

5. What is the purpose of a VPN?
   a) To encrypt data and provide secure remote access
   b) To block malicious websites
   c) To detect malware
   d) To monitor employee activity

Social Skills

6. How would you handle a situation where a colleague disagrees with your security recommendation?
   a) Ignore their opinion and proceed with your plan
   b) Escalate the issue to management immediately
   c) Listen to their concerns and collaborate on a solution
   d) Argue until they agree with you

7. What is the best way to communicate a security breach to non-technical stakeholders?
   a) Use technical jargon to explain the issue

b) Provide a high-level overview with clear impacts and actions
c) Avoid discussing the breach until it's fully resolved
d) Blame the IT team for the breach

8. How would you respond to a user who repeatedly falls for phishing scams?
   a) Report them to HR
   b) Provide additional training and resources
   c) Restrict their access to the internet
   d) Ignore the issue

9. What is the most important trait for a cybersecurity analyst when working in a team?
   a) Technical expertise
   b) Communication skills
   c) Independence
   d) Strict adherence to rules

10. How would you handle a situation where you discover a vulnerability but are asked to delay fixing it?
    a) Fix it immediately without approval
    b) Document the risk and escalate to management
    c) Ignore the vulnerability
    d) Resign from your position

Analysis and Problem-Solving

11. What is the first step in incident response?
    a) Contain the incident
    b) Identify the incident
    c) Eradicate the threat
    d) Recover systems

12. Which of the following is an example of a false positive in cybersecurity?
    a) A legitimate user is blocked by a firewall
    b) Malware is detected and removed
    c) A phishing email is flagged as spam
    d) A vulnerability is patched

13. What is the best way to prioritise vulnerabilities?
    a) Fix the easiest vulnerabilities first
    b) Use a risk-based approach (e.g., CVSS scores)
    c) Ignore vulnerabilities with low impact
    d) Fix vulnerabilities in the order they are discovered

14. What is the purpose of a SIEM system?
    a) Encrypt sensitive data
    b) Monitor and analyse security events in real-time
    c) Block malicious websites
    d) Scan for viruses

15. How would you investigate a sudden spike in network traffic?
    a) Assume it's normal and ignore it
    b) Check for signs of a DDoS attack or unauthorised access
    c) Restart the network devices
    d) Block all incoming traffic

Scenario-Based Questions

16. You receive an email from your CEO asking for an urgent wire transfer. What should you do?
    a) Process the transfer immediately
    b) Verify the request through a separate communication channel
    c) Ignore the email
    d) Reply to the email asking for more details

17. A user reports that their computer is running slowly. Upon investigation, you find unauthorised software installed. What is the next step?
    a) Reinstall the operating system
    b) Scan for malware and investigate further
    c) Ignore the issue
    d) Restart the computer

18. During a penetration test, you discover a critical vulnerability. What should you do first?
    a) Exploit the vulnerability to demonstrate the risk
    b) Report the vulnerability to the relevant team immediately
    c) Ignore the vulnerability
    d) Document the vulnerability but take no action

19. A colleague accidentally shares sensitive data on a public forum. What is the first step?
    a) Report the incident to HR
    b) Remove the data and assess the impact
    c) Ignore the incident
    d) Blame the colleague publicly

20. You notice unusual login attempts from an unknown IP address. What should you do?

a) Block the IP address immediately
b) Investigate further and monitor the activity
c) Ignore the activity
d) Change all user passwords

Technical Questions

21. What is the difference between symmetric and asymmetric encryption?
    a) Symmetric uses one key, asymmetric uses two keys
    b) Symmetric is faster, asymmetric is slower
    c) Symmetric is used for hashing, asymmetric for encryption
    d) Both use the same key

22. Which port is commonly used for SSH?
    a) 22
    b) 80
    c) 443
    d) 3389

23. What is the purpose of a honeypot?
    a) To attract and analyse attackers
    b) To encrypt sensitive data
    c) To block malicious traffic
    d) To monitor employee activity

24. Which of the following is a hashing algorithm?
    a) AES
    b) RSA
    c) SHA-256
    d) SSL

25. What is the primary function of a DNS server?
    a) Encrypt web traffic
    b) Translate domain names to IP addresses
    c) Block malicious websites
    d) Monitor network traffic

Advanced Technical Questions

26. What is the difference between IDS and IPS?
    a) IDS detects threats, IPS prevents them
    b) IDS prevents threats, IPS detects them
    c) Both are the same
    d) IDS is for networks, IPS is for endpoints

27. What is a zero-day vulnerability?
    a) A vulnerability that is exploited before a patch is available
    b) A vulnerability that has been patched
    c) A vulnerability with no known exploit
    d) A vulnerability in legacy systems

28. What is the purpose of a digital certificate?
    a) To encrypt data
    b) To verify the identity of a website or user
    c) To block malicious traffic
    d) To monitor network activity

29. Which of the following is an example of social engineering?
    a) Phishing
    b) DDoS attack
    c) SQL injection
    d) Cross-site scripting

30. What is the OWASP Top 10?
    a) A list of the most critical web application security risks
    b) A list of the most common malware types
    c) A list of the best cybersecurity tools
    d) A list of the top cybersecurity certifications

General Knowledge

31. What is the primary goal of a penetration test?
    a) To exploit vulnerabilities and gain unauthorised access
    b) To identify and fix vulnerabilities in a system
    c) To monitor network traffic
    d) To encrypt sensitive data

32. Which of the following is an example of multi-factor authentication (MFA)?
    a) Password and security question
    b) Password and fingerprint scan
    c) Password and CAPTCHA
    d) Password and email verification

33. What is the purpose of a disaster recovery plan (DRP)?
    a) To prevent cyberattacks
    b) To restore systems and data after a disruption
    c) To monitor employee activity
    d) To encrypt sensitive data

34. Which regulation is focused on protecting personal data in the European Union?
    a) HIPAA
    b) GDPR
    c) PCI DSS
    d) SOX

35. What is the primary purpose of a security policy?
    a) To define acceptable use of resources
    b) To encrypt sensitive data
    c) To block malicious websites
    d) To monitor network traffic

Social Skills

36. How would you explain the importance of cybersecurity to a non-technical executive?
    a) Use technical jargon to emphasize your expertise
    b) Focus on business risks and potential financial losses
    c) Avoid discussing cybersecurity unless asked
    d) Provide a detailed technical report

37. A team member is consistently missing deadlines. How would you address this?
    a) Report them to management immediately
    b) Offer support and ask if they need help
    c) Ignore the issue
    d) Publicly criticise their performance

38. How would you handle a situation where a manager asks you to bypass security protocols?
    a) Comply without question
    b) Explain the risks and suggest alternatives
    c) Ignore the request
    d) Report the manager to HR

39. What is the best way to build trust with your team?
    a) Take credit for their work
    b) Communicate openly and support their growth
    c) Avoid collaboration
    d) Micromanage their tasks

40. How would you respond to a user who is frustrated with frequent password changes?
    a) Ignore their frustration

b) Explain the importance of strong passwords and offer tips
c) Reduce the password complexity requirements
d) Report them to HR

Analysis and Problem-Solving

41. What is the first step in a risk assessment?
    a) Implement controls
    b) Identify assets and threats
    c) Monitor the network
    d) Encrypt sensitive data

42. Which of the following is an example of a preventive control?
    a) Firewall
    b) Incident response plan
    c) Backup and recovery plan
    d) Security awareness training

43. What is the purpose of a root cause analysis (RCA)?
    a) To identify the underlying cause of an incident
    b) To monitor network traffic
    c) To encrypt sensitive data
    d) To block malicious websites

44. How would you prioritise patching vulnerabilities in a large organisation?
    a) Patch all vulnerabilities at once
    b) Focus on critical vulnerabilities first
    c) Ignore vulnerabilities with low impact
    d) Patch vulnerabilities randomly

45. What is the best way to detect insider threats?
    a) Monitor user activity and behavior
    b) Block all external access
    c) Encrypt all data
    d) Restrict employee access to the internet

Scenario-Based Questions

46. A user reports that their account has been locked due to multiple failed login attempts. What should you do?
    a) Unlock the account immediately
    b) Investigate for potential brute force attacks
    c) Ignore the issue
    d) Change the user's password

47. During a routine scan, you discover an open port that should be closed. What is the next step?
    a) Close the port and investigate why it was open
    b) Ignore the issue
    c) Report the issue to management
    d) Block all incoming traffic

48. A phishing email is reported by multiple users. What should you do first?
    a) Delete the email from all inboxes
    b) Investigate the email and block the sender
    c) Ignore the issue
    d) Report the issue to HR

49. A critical system is infected with ransomware. What is the first step?
    a) Pay the ransom
    b) Isolate the system to prevent spread
    c) Reboot the system
    d) Ignore the issue

50. A vendor requests remote access to your network for maintenance. What should you do?
    a) Grant access immediately
    b) Verify the request and provide limited access
    c) Ignore the request
    d) Block the vendor's IP address

Technical Questions

51. What is the purpose of a salt in password hashing?
    a) To add randomness and prevent rainbow table attacks
    b) To encrypt the password
    c) To store the password in plaintext
    d) To block brute force attacks

52. Which protocol is used for email encryption?
    a) SMTP
    b) POP3
    c) IMAP
    d) S/MIME

53. What is the difference between a virus and a worm?
    a) A virus requires user interaction, a worm does not
    b) A worm requires user interaction, a virus does not

c) Both are the same
d) A virus spreads over networks, a worm does not

54. What is the purpose of a TPM (Trusted Platform Module)?
    a) To securely store encryption keys
    b) To monitor network traffic
    c) To block malicious websites
    d) To encrypt emails

55. Which of the following is a network reconnaissance tool?
    a) Nmap
    b) Wireshark
    c) Metasploit
    d) Nessus

Advanced Technical Questions

56. What is the difference between black-box and white-box testing?
    a) Black-box testing has no prior knowledge, white-box testing has full knowledge
    b) Black-box testing is for networks, white-box testing is for applications
    c) Both are the same
    d) Black-box testing is automated, white-box testing is manual

57. What is the purpose of a CSRF (Cross-Site Request Forgery) attack?
    a) To trick a user into performing actions without their consent
    b) To steal sensitive data
    c) To encrypt data
    d) To block access to a website

58. What is the primary function of a WAF (Web Application Firewall)?
    a) To protect web applications from attacks
    b) To encrypt web traffic
    c) To monitor network traffic
    d) To block malicious emails

59. What is the difference between steganography and cryptography?
    a) Steganography hides data, cryptography encrypts data
    b) Both are the same
    c) Steganography is for networks, cryptography is for applications
    d) Steganography encrypts data, cryptography hides data

60. What is the purpose of a security information and event management (SIEM) system?
    a) To monitor and analyse security events in real-time

b) To encrypt sensitive data
c) To block malicious websites
d) To scan for viruses

General Knowledge

61. What is the primary purpose of a security operations center (SOC)?
    a) To monitor and respond to security incidents
    b) To develop software applications
    c) To manage employee payroll
    d) To block malicious websites

62. Which of the following is an example of a physical security control?
    a) Firewall
    b) Security guards
    c) Antivirus software
    d) Encryption

63. What is the purpose of a data loss prevention (DLP) system?
    a) To prevent unauthorised access to sensitive data
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block malicious websites

64. Which of the following is NOT a common type of cyberattack?
    a) Phishing
    b) Ransomware
    c) Firewall
    d) DDoS

65. What is the primary purpose of a vulnerability assessment?
    a) To identify and prioritise vulnerabilities in a system
    b) To exploit vulnerabilities
    c) To monitor network traffic
    d) To encrypt sensitive data

Social Skills

66. How would you handle a situation where a team member is resistant to following security protocols?
    a) Report them to HR
    b) Explain the importance of the protocols and provide training
    c) Ignore the issue
    d) Publicly criticise their behavior

67. A stakeholder asks for a detailed technical report on a security incident. How would you respond?
    a) Provide a highly technical report without explanation
    b) Offer a high-level summary with technical details as an appendix
    c) Ignore the request
    d) Refuse to provide the report

68. How would you handle a situation where you discover a colleague has shared sensitive data externally?
    a) Report the incident to HR immediately
    b) Discuss the issue with the colleague and escalate if necessary
    c) Ignore the issue
    d) Publicly shame the colleague

69. What is the best way to handle a conflict with a team member over a security decision?
    a) Avoid the conflict and let them have their way
    b) Listen to their perspective and find a compromise
    c) Escalate the issue to management immediately
    d) Argue until they agree with you

70. How would you explain the importance of patching to a non-technical audience?
    a) Use technical jargon to emphasize the complexity
    b) Compare patching to fixing a leaky roof to prevent further damage
    c) Avoid discussing patching unless asked
    d) Provide a detailed technical report

Analysis and Problem-Solving

71. What is the purpose of a threat intelligence feed?
    a) To provide real-time information about emerging threats
    b) To encrypt sensitive data
    c) To block malicious websites
    d) To monitor employee activity

72. Which of the following is an example of a detective control?
    a) Intrusion detection system (IDS)
    b) Firewall
    c) Encryption
    d) Security awareness training

73. What is the primary purpose of a business impact analysis (BIA)?
    a) To identify critical business functions and their recovery priorities

b) To monitor network traffic
c) To encrypt sensitive data
d) To block malicious websites

74. How would you prioritise incidents in a SOC?
    a) First-come, first-served
    b) Based on severity and potential impact
    c) Ignore low-priority incidents
    d) Randomly

75. What is the purpose of a chain of custody in digital forensics?
    a) To ensure evidence is handled properly and remains admissible in court
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block malicious websites

Scenario-Based Questions

76. A user reports that their computer is displaying a ransomware message. What should you do first?
    a) Pay the ransom
    b) Isolate the computer from the network
    c) Reboot the computer
    d) Ignore the issue

77. During a security audit, you discover that a critical system has not been patched for months. What should you do?
    a) Patch the system immediately
    b) Report the issue to management and recommend a patching schedule
    c) Ignore the issue
    d) Blame the IT team

78. A phishing email is sent to all employees. What should you do first?
    a) Delete the email from all inboxes
    b) Investigate the email and notify employees
    c) Ignore the issue
    d) Report the issue to HR

79. A vendor's system is compromised and they have access to your network. What should you do?
    a) Terminate the vendor's contract immediately
    b) Revoke their access and investigate the breach
    c) Ignore the issue
    d) Block all external access

80. A critical vulnerability is discovered in a widely used software. What should you do first?
    a) Patch all systems immediately
    b) Assess the risk and prioritise patching
    c) Ignore the vulnerability
    d) Block all internet access

Technical Questions

81. What is the purpose of a MAC address?
    a) To uniquely identify a device on a network
    b) To encrypt data
    c) To block malicious websites
    d) To monitor network traffic

82. Which of the following is an example of a symmetric encryption algorithm?
    a) AES
    b) RSA
    c) ECC
    d) SHA-256

83. What is the purpose of a reverse proxy?
    a) To protect servers by handling client requests
    b) To encrypt data
    c) To block malicious websites
    d) To monitor network traffic

84. What is the difference between HTTP and HTTPS?
    a) HTTPS encrypts data, HTTP does not
    b) HTTP is faster, HTTPS is slower
    c) HTTP is for websites, HTTPS is for emails
    d) Both are the same

85. What is the purpose of a certificate authority (CA)?
    a) To issue and manage digital certificates
    b) To encrypt data
    c) To block malicious websites
    d) To monitor network traffic

Advanced Technical Questions

86. What is the purpose of a buffer overflow attack?
    a) To overwrite memory and execute malicious code

b) To encrypt data
c) To block malicious websites
d) To monitor network traffic

87. What is the difference between a false positive and a false negative in cybersecurity?
a) A false positive is a legitimate action flagged as malicious, a false negative is a malicious action not detected
b) Both are the same
c) A false positive is a malicious action not detected, a false negative is a legitimate action flagged as malicious
d) Both refer to undetected vulnerabilities

88. What is the purpose of a sandbox in cybersecurity?
a) To isolate and analyse suspicious files or programs
b) To encrypt data
c) To block malicious websites
d) To monitor network traffic

89. What is the difference between a vulnerability and an exploit?
a) A vulnerability is a weakness, an exploit is a tool or technique to take advantage of it
b) Both are the same
c) A vulnerability is a tool, an exploit is a weakness
d) Both refer to malware

90. What is the purpose of a security baseline?
a) To establish minimum security standards for systems
b) To encrypt data
c) To block malicious websites
d) To monitor network traffic

General Knowledge

91. What is the primary purpose of a demilitarised zone (DMZ) in network security?
a) To isolate public-facing servers from the internal network
b) To encrypt sensitive data
c) To block malicious websites
d) To monitor employee activity

92. Which of the following is an example of a security framework?
a) NIST Cybersecurity Framework
b) HTTP

c) TCP/IP
d) SMTP

93. What is the purpose of a security awareness training program?
    a) To educate employees about cybersecurity risks and best practices
    b) To encrypt sensitive data
    c) To block malicious websites
    d) To monitor network traffic

94. Which of the following is NOT a common authentication factor?
    a) Something you know (e.g., password)
    b) Something you have (e.g., token)
    c) Something you are (e.g., fingerprint)
    d) Something you want (e.g., desire)

95. What is the primary purpose of a security audit?
    a) To assess compliance with security policies and standards
    b) To encrypt sensitive data
    c) To block malicious websites
    d) To monitor network traffic

Scenario-Based Questions

96. A user reports that their account has been compromised. What should you do first?
    a) Reset the user's password and investigate the incident
    b) Ignore the issue
    c) Report the issue to HR
    d) Block the user's account permanently

97. During a routine scan, you discover that a server is running an outdated operating system. What should you do?
    a) Upgrade the operating system immediately
    b) Document the risk and plan an upgrade
    c) Ignore the issue
    d) Block the server from the network

98. A phishing email is sent to a small group of employees. What should you do first?
    a) Delete the email from all inboxes
    b) Investigate the email and notify the affected employees
    c) Ignore the issue
    d) Report the issue to HR

99. A critical vulnerability is discovered in a third-party software used by your organisation. What should you do first?

a) Patch the software immediately
b) Assess the risk and contact the vendor for a patch
c) Ignore the vulnerability
d) Block all internet access

100. A user accidentally downloads a malicious file. What should you do first?
a) Isolate the user's computer and scan for malware
b) Ignore the issue
c) Report the issue to HR
d) Reboot the user's computer

Technical Questions

101. What is the purpose of a network access control (NAC) system?
a) To enforce security policies on devices connecting to the network
b) To encrypt sensitive data
c) To block malicious websites
d) To monitor network traffic

102. Which of the following is an example of a network protocol?
a) TCP/IP
b) AES
c) SHA-256
d) RSA

103. What is the purpose of a security information and event management (SIEM) system?
a) To monitor and analyse security events in real-time
b) To encrypt sensitive data
c) To block malicious websites
d) To scan for viruses

104. What is the difference between a vulnerability scan and a penetration test?
a) A vulnerability scan identifies weaknesses, a penetration test exploits them
b) Both are the same
c) A vulnerability scan exploits weaknesses, a penetration test identifies them
d) Both refer to malware detection

105. What is the purpose of a security baseline?
a) To establish minimum security standards for systems
b) To encrypt data
c) To block malicious websites
d) To monitor network traffic

Answers

1. a) Confidentiality, Integrity, Availability
2. c) Firewall
3. b) Monitor network traffic and block unauthorised access
4. c) HTTPS
5. a) To encrypt data and provide secure remote access
6. c) Listen to their concerns and collaborate on a solution
7. b) Provide a high-level overview with clear impacts and actions
8. b) Provide additional training and resources
9. b) Communication skills
10. b) Document the risk and escalate to management
11. b) Identify the incident
12. a) A legitimate user is blocked by a firewall
13. b) Use a risk-based approach (e.g., CVSS scores)
14. b) Monitor and analyse security events in real-time
15. b) Check for signs of a DDoS attack or unauthorised access
16. b) Verify the request through a separate communication channel
17. b) Scan for malware and investigate further
18. b) Report the vulnerability to the relevant team immediately
19. b) Remove the data and assess the impact
20. b) Investigate further and monitor the activity
21. a) Symmetric uses one key, asymmetric uses two keys
22. a) 22
23. a) To attract and analyse attackers
24. c) SHA-256
25. b) Translate domain names to IP addresses
26. a) IDS detects threats, IPS prevents them
27. a) A vulnerability that is exploited before a patch is available
28. b) To verify the identity of a website or user
29. a) Phishing
30. a) A list of the most critical web application security risks
31. b) To identify and fix vulnerabilities in a system
32. b) Password and fingerprint scan
33. b) To restore systems and data after a disruption
34. b) GDPR
35. a) To define acceptable use of resources
36. b) Focus on business risks and potential financial losses
37. b) Offer support and ask if they need help
38. b) Explain the risks and suggest alternatives
39. b) Communicate openly and support their growth
40. b) Explain the importance of strong passwords and offer tips
41. b) Identify assets and threats
42. a) Firewall

43. a) To identify the underlying cause of an incident
44. b) Focus on critical vulnerabilities first
45. a) Monitor user activity and behavior
46. b) Investigate for potential brute force attacks
47. a) Close the port and investigate why it was open
48. b) Investigate the email and block the sender
49. b) Isolate the system to prevent spread
50. b) Verify the request and provide limited access
51. a) To add randomness and prevent rainbow table attacks
52. d) S/MIME
53. a) A virus requires user interaction, a worm does not
54. a) To securely store encryption keys
55. a) Nmap
56. a) Black-box testing has no prior knowledge, white-box testing has full knowledge
57. a) To trick a user into performing actions without their consent
58. a) To protect web applications from attacks
59. a) Steganography hides data, cryptography encrypts data
60. a) To monitor and analyse security events in real-time
61. a) To monitor and respond to security incidents
62. b) Security guards
63. a) To prevent unauthorised access to sensitive data
64. c) Firewall
65. a) To identify and prioritise vulnerabilities in a system
66. b) Explain the importance of the protocols and provide training
67. b) Offer a high-level summary with technical details as an appendix
68. b) Discuss the issue with the colleague and escalate if necessary
69. b) Listen to their perspective and find a compromise
70. b) Compare patching to fixing a leaky roof to prevent further damage
71. a) To provide real-time information about emerging threats
72. a) Intrusion detection system (IDS)
73. a) To identify critical business functions and their recovery priorities
74. b) Based on severity and potential impact
75. a) To ensure evidence is handled properly and remains admissible in court
76. b) Isolate the computer from the network
77. b) Report the issue to management and recommend a patching schedule
78. b) Investigate the email and notify employees
79. b) Revoke their access and investigate the breach
80. b) Assess the risk and prioritise patching
81. a) To uniquely identify a device on a network
82. a) AES
83. a) To protect servers by handling client requests
84. a) HTTPS encrypts data, HTTP does not
85. a) To issue and manage digital certificates
86. a) To overwrite memory and execute malicious code

87. a) A false positive is a legitimate action flagged as malicious, a false negative is a malicious action not detected
88. a) To isolate and analyse suspicious files or programs
89. a) A vulnerability is a weakness, an exploit is a tool or technique to take advantage of it
90. a) To establish minimum security standards for systems
91. a) To isolate public-facing servers from the internal network
92. a) NIST Cybersecurity Framework
93. a) To educate employees about cybersecurity risks and best practices
94. d) Something you want (e.g., desire)
95. a) To assess compliance with security policies and standards
96. a) Reset the user's password and investigate the incident
97. b) Document the risk and plan an upgrade
98. b) Investigate the email and notify the affected employees
99. b) Assess the risk and contact the vendor for a patch
100. a) Isolate the user's computer and scan for malware
101. a) To enforce security policies on devices connecting to the network
102. a) TCP/IP
103. a) To monitor and analyse security events in real-time
104. a) A vulnerability scan identifies weaknesses, a penetration test exploits them
105. a) To establish minimum security standards for systems