GIAC

GNFA

GIAC Network Forensic Analyst (GNFA)

Questions&AnswersPDF

Latest Version: 6.0

Question: 1

What methods are used to identify the structure of an unknown network protocol?
(Select two.)
Response:

A. Static code analysis
B. Packet inspection
C. Watching video tutorials
D. Reverse engineering binaries

Answer: B,D

Question: 2

Which field in a NetFlow record can help determine if lateral movement is occurring within a network?
Response:

A. Protocol Type
B. Destination IP Address
C. Source and Destination Port
D. Destination IP Address and Source and Destination Port

Answer: D

Question: 3

You are analyzing network traffic and find a series of communications using an unknown protocol. The traffic appears structured, but there is no official documentation available. What should be your first step?
Response:

A. Capture and inspect the packets using Wireshark
B. Attempt brute-force decryption
C. Block all traffic using the protocol immediately
D. Search for open-source documentation

Answer: A

Question: 4

An organization notices an increase in wireless network congestion and connectivity issues. What steps should be taken to identify potential sources of interference?
Response:

A. Conduct a site survey to identify interference sources
B. Increase the power of the access points
C. Disable WPA2 encryption
D. Implement VLAN segmentation

Answer: A

Question: 5

Which best practices should organizations follow when configuring log retention policies? (Select two.)
Response:

A. Store all logs indefinitely
B. Encrypt logs to prevent unauthorized access
C. Retain logs based on regulatory compliance requirements
D. Delete all logs after 30 days to save storage space

Answer: B,C

Question: 6

Your company is implementing a Zero Trust network model. Which approach would best align with Zero Trust principles?
Response:

A. Granting access based on IP address
B. Requiring continuous authentication and strict access controls
C. Using only perimeter-based firewalls
D. Allowing unrestricted lateral movement within the network

Answer: B

Question: 7

Which open-source tool is commonly used as a forward and reverse proxy for security analysis?
Response:

A. Burp Suite
B. Snort
C. Wireshark
D. Nessus

Answer: A

Question: 8

A security analyst is tasked with identifying unauthorized devices connecting to a company's Wi-Fi network. What is the best approach to detecting unauthorized connections?
Response:

A. Using Nmap to scan open ports
B. Enabling WPA3 authentication
C. Monitoring MAC addresses in the access point logs
D. Disabling SSID broadcasting

Answer: C

Question: 9

Which of the following encoding methods is most commonly used to represent binary data in text format?
Response:

A. Base64
B. SHA-256
C. XOR
D. Blowfish

Answer: A

Question: 10

What are potential indicators of malicious network activity in an unknown protocol?
(Select two.)
Response:

A. Repeated failed login attempts
B. Large encrypted data transfers to unknown IPs
C. Use of TLS encryption
D. Traffic on well-known service ports

Answer: A,B