GIAC.GNFA.v2026-07-16.q39

Exam Code:	GNFA
Exam Name:	GIAC Network Forensic Analyst (GNFA)
Certification Provider:	GIAC
Free Question Number:	39
Version:	v2026-07-16
# of views:	106
# of Questions views:	404
https://www.freecram.net/torrent/GIAC.GNFA.v2026-07-16.q39.html	

NEW QUESTION: 1
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: (SHOW ANSWER)

NEW QUESTION: 2
Which network security proxy tool is commonly used to analyze and modify HTTPS traffic?
Response:
A. Nmap
B. Snort
C. MITMProxy
D. Squid Proxy
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which of the following are characteristics of symmetric encryption?
(Select two.)
Response:
A. Uses a shared secret key
B. Faster than asymmetric encryption
C. Uses digital signatures for verification
D. Requires a public-private key pair

Answer: (SHOW ANSWER)

NEW QUESTION: 4
Which of the following is a common use case for a reverse proxy?
Response:
A. Blocking outbound web requests
B. Enhancing security by hiding backend servers
C. Encrypting internal DNS queries
D. Bypassing firewall policies
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which tool is commonly used for reverse engineering network protocols by capturing and analyzing packet data?
Response:
A. Metasploit
B. Wireshark
C. Nmap
D. Netcat
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
An organization suspects that an attacker is using a tunneling technique to evade detection. The analyst checks NetFlow records and sees a high number of outbound DNS queries with unusually large payloads. What type of attack is likely occurring?
Response:
A. DDoS attack
B. Man-in-the-Middle attack
C. Ransomware execution
D. DNS Exfiltration
Answer: (SHOW ANSWER)

NEW QUESTION: 7
A network administrator notices that an internal web server is being accessed from multiple external sources in an unusual pattern. What security proxy feature would help in identifying and mitigating this attack?
Response:
A. Data compression
B. Application-layer filtering
C. DNS caching
D. Port forwarding

Answer: (SHOW ANSWER)

NEW QUESTION: 8
Which open-source tools are commonly used for network security proxying?
(Select two.)
Response:
A. Privoxy
B. OpenVPN
C. Wireshark
D. Squid
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which of the following are security risks associated with FTP?
(Select two.)
Response:
A. Data is transmitted in plaintext
B. It lacks built-in encryption
C. It is limited to local file transfers only
D. It is a UDP-based protocol
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following best describes asymmetric encryption?
Response:

A. Uses a predefined lookup table for encoding data
B. Uses the same key for encryption and decryption
C. Uses different keys for encryption and decryption
D. Converts plaintext into a hash that cannot be reversed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
What are the main functions of the Domain Name System (DNS)?
(Select two.)
Response:
A. Assigning MAC addresses to devices
B. Managing email servers
C. Resolving domain names to IP addresses
D. Distributing network traffic among multiple servers
Answer: (SHOW ANSWER)

NEW QUESTION: 12
What is the primary purpose of a VLAN in network architecture?
Response:
A. To replace firewalls in enterprise environments
B. To encrypt network traffic
C. To logically segment networks without requiring physical separation
D. To increase network speed
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which of the following hashing algorithms is considered weak due to its vulnerability to collisions?
Response:
A. AES-256
B. MD5
C. RSA-2048
D. SHA-512
Answer: (SHOW ANSWER)

NEW QUESTION: 14
What are potential indicators of malicious network activity in an unknown protocol?
(Select two.)
Response:
A. Repeated failed login attempts
B. Use of TLS encryption
C. Large encrypted data transfers to unknown IPs
D. Traffic on well-known service ports
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which of the following best describes an SIEM (Security Information and Event Management) system?
Response:
A. A device that encrypts all logs for security purposes
B. A firewall rule enforcement mechanism
C. A system that collects, normalizes, and analyzes security logs
D. A tool that blocks malicious network traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 16

An administrator notices unusual traffic patterns where a single workstation is attempting to connect to multiple internal servers within minutes. What should be the first step in investigating this activity?
Response:
A. Review network segmentation policies
B. Block all outbound connections from the workstation
C. Analyze the NetFlow records and IDS alerts
D. Disable the workstation immediately
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following are features of a forward proxy?
(Select two.)
Response:
A. Caches frequently accessed web content
B. Filters outgoing client requests
C. Functions only at the transport layer
D. Protects internal servers from direct exposure
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which NetFlow version is most commonly used for advanced traffic analysis in modern networks?
Response:
A. NetFlow v1
B. NetFlow v5
C. NetFlow v7
D. NetFlow v9
Answer: (SHOW ANSWER)

NEW QUESTION: 19
A security analyst observes multiple failed login attempts from the same IP address within a short time. What is the most appropriate action to take?

Response:

A. Investigate the source IP and check for additional related logs

B. Delete the logs to free up storage space

C. Ignore the event unless a successful login occurs

D. Block the IP address immediately

Answer: (SHOW ANSWER)

NEW QUESTION: 20

Which of the following can be used to detect rogue access points in a wireless network?

Response:

A. NetFlow

B. Wireshark

C. Wireless Intrusion Detection System (WIDS)

D. Syslog

Answer: (SHOW ANSWER)

NEW QUESTION: 21

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: (SHOW ANSWER)

NEW QUESTION: 22

What are common characteristics of rogue access points?

(Select two.)

Response:

A. They always use enterprise-level encryption

B. They broadcast unauthorized SSIDs

C. They can be used for phishing attacks

D. They only exist in wired networks

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 23

Which tools are useful for network protocol reverse engineering?

(Select two.)

Response:

A. IDA Pro

B. Nessus
C. Kali Linux
D. Wireshark
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Which of the following best describes a NetFlow record?
Response:
A. A complete capture of all packets in a session
B. A database of encrypted network payloads
C. A list of blocked IP addresses in a firewall
D. A summary of network communication between hosts
Answer: (SHOW ANSWER)

NEW QUESTION: 25
What is the main advantage of a segmented network architecture?
Response:
A. Elimination of network monitoring needs
B. Improved security by limiting lateral movement
C. Reduced performance due to additional firewalls
D. Increased complexity in routing
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which of the following NetFlow-based anomalies could indicate a Distributed Denial-of-Service (DDoS) attack?
(Select two.)
Response:
A. Unusual encrypted payload patterns
B. Large number of failed login attempts
C. High number of unique destination IPs from a single source
D. High volume of traffic from a single source
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which protocol is commonly used for network device management and monitoring?
Response:
A. FTP
B. DHCP
C. HTTP
D. SNMP

Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which of the following protocols provides secure file transfers by encrypting data during transmission?
Response:
A. SFTP
B. Telnet
C. HTTP
D. FTP
Answer: (SHOW ANSWER)

NEW QUESTION: 29
What is the primary security concern associated with HTTP compared to HTTPS?
Response:
A. HTTP transmits data in plaintext
B. HTTP requires additional bandwidth
C. HTTP requires certificates for authentication
D. HTTP has a slower connection speed
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Which benefits do security proxies provide in enterprise environments? (Select two.)
Response:

A. Preventing all phishing attacks
B. Content filtering and malware detection
C. Logging and monitoring network traffic
D. Reducing network latency
Answer: (SHOW ANSWER)

NEW QUESTION: 31
An attacker intercepts a legitimate communication session and inserts malicious commands while appearing as a trusted participant. Which protocol is most vulnerable to this attack due to its lack of encryption?
Response:
A. HTTPS
B. SFTP
C. SSH
D. FTP
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which of the following log sources would be most useful for detecting brute-force login attempts?
Response:
A. DNS query logs
B. Network firewall logs
C. Authentication logs
D. Web server access logs
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following are key benefits of centralizing security event logs?
(Select two.)
Response:
A. Immediate compliance with all security regulations
B. Faster network speeds
C. Reduced need for manual log review
D. Improved detection of correlated security events
Answer: (SHOW ANSWER)

NEW QUESTION: 34
What is the primary purpose of NetFlow in network security analysis?
Response:
A. Encrypting network traffic to prevent data leaks
B. Blocking malicious IPs automatically
C. Monitoring and analyzing network traffic patterns
D. Capturing full packet data for forensic analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which of the following network components is responsible for enforcing security policies between different network segments?

Response:
A. Router
B. Load Balancer
C. Firewall
D. Switch
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
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. Disabling SSID broadcasting
B. Monitoring MAC addresses in the access point logs
C. Enabling WPA3 authentication
D. Using Nmap to scan open ports
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which of the following encryption algorithms are considered secure for modern cryptographic use?
(Select two.)
Response:
A. AES-256
B. RC4
C. DES
D. Blowfish
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Which security measures help protect against unauthorized access to network architecture?
(Select two.)
Response:
A. Using default admin credentials
B. Deploying intrusion detection systems (IDS)
C. Allowing open access to all internal systems
D. Implementing least privilege access
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 39
What is a key advantage of using a proxy-based firewall compared to a packet-filtering firewall?
Response:

A. Proxy-based firewalls cannot block specific content types
B. Proxy-based firewalls inspect entire application-layer data
C. Packet-filtering firewalls are more secure
D. Packet-filtering firewalls work at the application layer
Answer: (SHOW ANSWER)