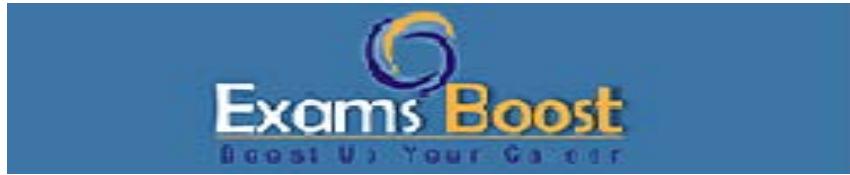


Boost up Your Certification Score

GIAC **GNFA**

GIAC Network Forensic Analyst (GNFA)



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

Which protocol is commonly used for network device management and monitoring?

Response:

- A. HTTP
- B. SNMP
- C. FTP
- D. DHCP

Answer: B

Question: 2

Which security measures help protect against unauthorized access to network architecture?

(Select two.)

Response:

- A. Implementing least privilege access
- B. Using default admin credentials
- C. Deploying intrusion detection systems (IDS)
- D. Allowing open access to all internal systems

Answer: A,C

Question: 3

Which technologies are commonly used in network segmentation strategies?

(Select two.)

Response:

- A. VLANs
- B. MPLS
- C. IPv6
- D. VPN

Answer: A,B

Question: 4

What is the primary purpose of a VLAN in network architecture?

Response:

- A. To increase network speed
- B. To logically segment networks without requiring physical separation
- C. To encrypt network traffic
- D. To replace firewalls in enterprise environments

Answer: B

Question: 5

Which challenges are commonly encountered when reverse engineering network protocols?

(Select two.)

Response:

- A. Lack of documentation
- B. Presence of encryption
- C. Use of default ports
- D. Standardized communication patterns

Answer: A,B

Question: 6

Which of the following is an indication of a custom or proprietary network protocol?

Response:

- A. Standard TCP and UDP port usage
- B. Non-standard packet structures and headers
- C. Use of open-source encryption libraries
- D. Presence of cleartext credentials in packets

Answer: B

Question: 7

Which actions can be taken after detecting malicious activity using NetFlow?

(Select two.)

Response:

- A. Block malicious IP addresses at the firewall
- B. Capture full packet data for forensic analysis
- C. Decrypt all traffic for deeper analysis
- D. Modify encryption keys dynamically

Answer: A,B

Question: 8

Which of the following are key benefits of centralizing security event logs?

(Select two.)

Response:

- A. Improved detection of correlated security events
- B. Reduced need for manual log review
- C. Faster network speeds
- D. Immediate compliance with all security regulations

Answer: A,B

Question: 9

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: 10

A security analyst detects an application sending large volumes of encoded traffic to a remote server over an uncommon port. The analyst suspects data exfiltration. What should be done next?

Response:

- A. Investigate the encoding scheme used in the traffic
- B. Immediately block the port on the firewall
- C. Assume the traffic is normal and ignore it
- D. Terminate all active network sessions

Answer: A

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**

