

Boost up Your Certification Score

GIAC **GAWN**

GIAC Assessing and Auditing Wireless Networks



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

What are the recommended practices for securing WPA3-enabled networks?

(Choose Three)

Response:

- A. Disabling WPS
- B. Using strong, unique passwords
- C. Limiting the use of legacy protocols
- D. Enabling MAC address filtering
- E. Regular firmware updates

Answer: A,B,E

Question: 2

What is the typical attack vector used to compromise high-frequency RFID systems?

Response:

- A. Signal jamming
- B. Eavesdropping
- C. SQL injection
- D. Phishing

Answer: B

Question: 3

During an advanced fuzzing attack, what is the primary objective when targeting an 802.11 network?

Response:

- A. Capturing handshakes
- B. Forcing reconnections
- C. Causing denial of service
- D. Decrypting traffic

Answer: C

Question: 4

In practical SDR applications, what is crucial for maintaining operational security while conducting wireless analyses?

Response:

- A. Keeping the SDR device physically secure
- B. Only analyzing publicly available frequencies
- C. Conducting operations during off-peak hours
- D. Using directional antennas to limit the reception range

Answer: A

Question: 5

What is a common vulnerability in Bluetooth technology that allows unauthorized access through brute force attacks?

Response:

- A. Bluejacking
- B. Bluesnarfing
- C. Bluebugging
- D. BlueSmacking

Answer: C

Question: 6

Which scenarios are indicative of a rogue network setup?

(Choose Two)

Response:

- A. A network with a slightly different SSID from the legitimate one
- B. A network offering unusually high data speeds
- C. A network using the same SSID but weaker encryption
- D. A network that appears and disappears frequently

Answer: A,D

Question: 7

How can wireless client segmentation reduce security risks?

Response:

- A. By limiting the broadcast domain
- B. By reducing signal strength
- C. By encrypting data on the network
- D. By isolating client devices from the core network

Answer: D

Question: 8

NFC transactions, what security mechanism is often employed to protect data integrity and confidentiality?

Response:

- A. Frequency hopping
- B. Transport Layer Security (TLS)
- C. Data masking
- D. Secure element (SE)

Answer: D

Question: 9

Which of the following are vulnerabilities specific to WPA2 that are addressed in WPA3?

(Choose Two)

Response:

- A. Susceptibility to KRACK
- B. Vulnerability to dictionary attacks
- C. Poor scalability in enterprise environments
- D. Lack of support for Fast BSS Transition (FT)

Answer: A,B

Question: 10

Which method is commonly used to audit the security of a hotspot?

Response:

- A. Checking for physical security breaches
- B. Monitoring network traffic for anomalies
- C. Ensuring all users have updated antivirus software
- D. Regularly changing Wi-Fi passwords

Answer: B

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**

