



GPEN^{Q&As}

GIAC Certified Penetration Tester

Pass GIAC GPEN Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/gpen.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

Which of the following tools is John using to crack the wireless encryption keys?

- A. Kismet
- B. AirSnort
- C. Cain
- D. PsPasswd

Correct Answer: B

QUESTION 2

In which of the following attacks does an attacker use packet sniffing to read network traffic between two parties to steal the session cookie?

- A. Cross-site scripting
- B. Session sidejacking
- C. ARP spoofing
- D. Session fixation

Correct Answer: B

QUESTION 3

GSM uses either A5/1 or A5/2 stream cipher for ensuring over-the-air voice privacy. Which of the following cryptographic attacks can be used to break both ciphers?

- A. Man-in-the-middle attack
- B. Ciphertext only attack
- C. Known plaintext attack
- D. Replay attack



Correct Answer: B

QUESTION 4

Which of the following tools is based on the SATAN tool?

- A. Retina
- B. Internet scanner
- C. GFI LANguard
- D. SAINT

Correct Answer: D

QUESTION 5

You suspect that a firewall or IPS exists between you and the target machine. Which nmap option will elicit responses from some firewalls and IPSs while being silently dropped by the target, thus confirming the existence of a firewall or IPS?

- A. -Traceroute
- B. -Firewalk
- C. -Badsum
- D. --SF

Correct Answer: B

[GPEN PDF Dumps](#)

[GPEN Practice Test](#)

[GPEN Braindumps](#)