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.geekcert.com/gpen.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?

A. Post-attack phase

B. Attack phase

C. On-attack phase

D. Pre-attack phase

Correct Answer: D

QUESTION 2

Which of the following is the feature that separates the use of Rainbow Tables from other applications such as Cain or John the Ripper?

A. Salts are used to create massive password databases for comparison.

B. Applications take advantage of 64-bit CPU processor and multithread the crackingprocess.

C. Data Is aligned efficiently in the rainbow tables making the search process quicker

D. Raw hashed passwords are compared to pre-calculated hash tables.

Correct Answer: B

QUESTION 3

Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system. Which of the following are the most likely threats to his computer? Each correct answer represents a complete solution. Choose two.

A. Attacker by creating a fake wireless network with high power antenna cause Victor\\'s computer to associate with his network to gain access.

B. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.

C. Attacker can use the Ping Flood DoS attack if WZC is used.

D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

Correct Answer: AB

QUESTION 4

You are conducting a penetration test for a private company located in the UK. The scope extends to all internal and external hosts controlled by the company. You have gathered necessary hold-harmless and non-disclosure agreements. Which action by your group can incur criminal liability under the computer Misuse Act of 1990?

A. Sending crafted packets to internal hosts in an attempt to fingerprint the operatingsystems

B. Recovering the SAM database of the domain server and attempting to crackpasswords

C. Installing a password sniffing program on an employee\\'s personal computer withoutconsent

D. Scanning open ports on internal user workstations and exploiting vulnerableapplications

Correct Answer: B

QUESTION 5

You\\'ve been asked to test a non-transparent proxy lo make sure it is working. After confirming the browser is correctly pointed at the proxy, you try to browse a web site. The browser indicates it is "loading" but never displays any part the page. Checking the proxy, you see a valid request in the proxy from your browser. Checking the response to the proxy, you see the results displayed in the accompanying screenshot. Which of the following answers is the most likely reason the browser hasn\\'t displayed the page yet?

A. The proxy is likely hung and must be restarted.

B. The proxy is configured to trap responses.

C. The proxy is configured to trap requests.

D. The site you are trying to reach is currently down.

Correct Answer: C