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.passapply.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

Which of the following tools connects to and executes files on remote systems?

A. Spector

B. Hk.exe

C. PsExec

D. GetAdmin.exe

Correct Answer: C

QUESTION 2

Which of the following tools can be used to enumerate networks that have blocked ICMP Echo packets, however, failed to block timestamp or information packet or not performing sniffing of trusted addresses, and it also supports spoofing and promiscuous listening for reply packets?

A. Nmap

B. Zenmap

C. Icmpenum

D. Nessus

Correct Answer: C

QUESTION 3

You send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024 using hping2 utility. This attack is known as _____.

A. Port scanning

B. Spoofing

C. Cloaking

D. Firewalking

Correct Answer: D

QUESTION 4

In which of the following attacks is a malicious packet rejected by an IDS, but accepted by the host system?

A. Insertion

B. Evasion

C. Fragmentation overwrite

D. Fragmentation overlap

Correct Answer: B

QUESTION 5

Which of the following can be used as a countermeasure against the SQL injection attack? Each correct answer represents a complete solution. Choose two.

A. mysql_real_escape_string()

B. Prepared statement

C. mysql_escape_string()

D. session_regenerate_id()

Correct Answer: AB