GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

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

https://www.passapply.com/gcih.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 types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack

B. Replay attack

C. Teardrop attack

D. Land attack

Correct Answer: A

QUESTION 2

An analyst runs the following nmap scan from their Linux computer as a non-privileged user. The target host, 10.0.233.2, has tcp/445 open. What network traffic would be generated by this scan?

$ nmap 10.0.233.2

A. ICMP echo and reply between the source and destination

B. No traffic will be captured as the scan is passive

C. TCP handshake between the source and destination hosts

D. ACK packets from the source to the destination

Correct Answer: C

A basic nmap scan, when not running as root, does a full TCP connect scan and completes the 3-way handshake.

QUESTION 3

Following the recent acquisition of a new business, your manager asks you to investigate their DNS service and report back on its status. He is concerned as they only have one DNS server in the organization and it is visible on the Internet. What actions and recommendations should be taken as a first step?

A. Review the logs of the acquired business\\' firewall for port 53 traffic. Add a firewall rule to block port 53 traffic.

B. Ensure zone transfer requests from the acquired business\\' DNS server are disabled. Propose a plan to migrate the DNS service to your split-DNS infrastructure.

C. Use the nslookup command to direct the aquired business\\' DNS server to transfer its records to your primary DNS server. Block all other traffic at the firewall.

D. Remove the acquired business\\' DNS server from the network. Import its database entries into your secure infrastructure.

Correct Answer: A

QUESTION 4

FILL BLANK

Fill in the blank with the appropriate word.

StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft\\'s /GS option use _____ defense against buffer overflow attacks.

A.

B.

C.

D.

Correct Answer:

QUESTION 5

Which of the following methods can be used to detect session hijacking attack?

A. nmap

B. Brutus

C. ntop

D. sniffer

Correct Answer: D