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.pass2lead.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 tools can be used for stress testing of a Web server? Each correct answer represents a complete solution. (Choose two.)

A. Internet bots

B. Scripts

C. Anti-virus software

D. Spyware

Correct Answer: AB

QUESTION 2

Which of the following is the method of hiding data within another media type such as graphic or document?

A. Spoofing

B. Steganography

C. Packet sniffing

D. Cryptanalysis

Correct Answer: B

QUESTION 3

You are an incident handler from a Fortune 500 oil and gas company. While reviewing the Data Loss Prevention (DLP) email software alerts, you find an email with Personally Identifiable Information (PII) in an attachment. The email is listed

below.

"From: John Smith

To: Frank Esler

Sub: Stuff

Frank, enclosed is the data you asked for. I will be sending you my bank details shortly for you to deposit the money that we discussed.

Attachment: Stuff.doc"

When analyzing the attachment, you discovered that the document had detailed information on the budget, the companies that your corporation is going to acquire within the next quarter along with the personal information of the individuals

who are involved in the purchase. You had determined that the DLP alert was based on a signature that alerted on a phone number typo that was formatted like a social security number in the document. How would you proceed with your analysis in this situation?

A. Do not report this, since it was a false alarm by the DLP software and there was no PII enclosed

B. Do not report this, since I know Frank and he would not use this information even if emailed to him

C. Report this as a probable malware incident, since the "stuff.doc" file looks suspicious

D. Report this as a possible insider threat incident, since John has sent out confidential information

Correct Answer: D

QUESTION 4

Which of the following Metasploit module types would contain privilege escalation capabilities?

A. Auxiliary

B. Exploit

C. Post

D. Payload

Correct Answer: D

Reference: https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/

QUESTION 5

Which of the following is recommended to include in your incident response jump bag?

A. A switch, because they will not route malicious arp packets

B. A hub, because they are far more reliable than switches

C. A router, because they enable you to monitor a network without being detected

D. A TAP, because you cannot easily sniff network traffic through a switch

Correct Answer: B