GCED Q&As

GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

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

https://www.passapply.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Michael, a software engineer, added a module to a banking customer\\'s code. The new module deposits small amounts of money into his personal bank account. Michael has access to edit the code, but only code reviewers have the ability to commit modules to production. The code reviewers have a backlog of work, and are often willing to trust the software developers\\' testing and confidence in the code.

Which technique is Michael most likely to engage to implement the malicious code?

A. Denial of Service

B. Race Condition

C. Phishing

D. Social Engineering

Correct Answer: C

QUESTION 2

Why might an administrator not be able to delete a file using the Windows del command without specifying additional command line switches?

A. Because it has the read-only attribute set

B. Because it is encrypted

C. Because it has the nodel attribute set

D. Because it is an executable file

Correct Answer: A

QUESTION 3

Which type of media should the IR team be handling as they seek to understand the root cause of an incident?

A. Restored media from full backup of the infected host

B. Media from the infected host, copied to the dedicated IR host

C. Original media from the infected host

D. Bit-for-bit image from the infected host

Correct Answer: A

Explanation: By imaging the media with tools such as dd or Ghost and analyzing the copy, you preserve the original media for later analysis so that the results can be recreated by another competent examiner if necessary.

QUESTION 4

Following a Digital Forensics investigation, which of the following should be included in the final forensics report?

A. An executive summary that includes a list of all forensic procedures performed.

B. A summary of the verified facts of the incident and the analyst\\'s unverified opinions.

C. A summary of the incident and recommended disciplinary actions to apply internally.

D. An executive summary that includes high level descriptions of the overall findings.

Correct Answer: D

Explanation: A professional forensic report should include an executive summary, including a description of the incident and the overall findings.

The written report needs to be factually accurate and free from speculation or bias, meaning that an analyst\\'s unverified or unsubstantiated opinions should not be included in the report. Beyond the executive summary, the detailed report should include a description of the data preserved, a detailed explanation of the procedures performed, and a summary of the facts. Disciplinary action, if needed, would be addressed

through other channels and not included in the forensic analyst\\'s report.

QUESTION 5

The creation of a filesystem timeline is associated with which objective?

A. Forensic analysis

B. First response

C. Access control

D. Incident eradication

Correct Answer: A