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

An internal host at IP address 10.10.50.100 is suspected to be communicating with a command and control whenever a user launches browser window. What features and settings of Wireshark should be used to isolate and analyze this network traffic?

A. Filter traffic using ip.src = = 10.10.50.100 and tcp.srcport = = 80, and use Expert Info

B. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 53, and use Expert Info

C. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 80, and use Follow TCP stream

D. Filter traffic using ip.src = = 10.10.50.100, and use Follow TCP stream

Correct Answer: C

QUESTION 2

Which of the following is considered a preventative control in operational security?

A. Smoke Sensors

B. Fire Suppressant

C. Voltage Regulators

D. Vibration Alarms

Correct Answer: B

Explanation: A fire suppressant device is a preventive control. Smoke sensors, vibration alarms, and voltage regulators are part of detection controls.

QUESTION 3

Before re-assigning a computer to a new employee, what data security technique does the IT department use to make sure no data is left behind by the previous user?

A. Fingerprinting

B. Digital watermarking

C. Baselining

D. Wiping

Correct Answer: D

QUESTION 4

Which of the following is best defined as "anything that has the potential to target known or existing vulnerabilities in a system?"

A. Vector

B. Gateway

C. Threat

D. Exploit

Correct Answer: A

QUESTION 5

What is the BEST sequence of steps to remove a bot from a system?

A. Terminate the process, remove autoloading traces, delete any malicious files

B. Delete any malicious files, remove autoloading traces, terminate the process

C. Remove autoloading traces, delete any malicious files, terminate the process

D. Delete any malicious files, terminate the process, remove autoloading traces

Correct Answer: A