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.pass4itsure.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

Of the following pieces of digital evidence, which would be collected FIRST from a live system involved in an incident?

A. Event logs from a central repository

B. Directory listing of system files

C. Media in the CDrom drive

D. Swap space and page files

Correct Answer: D

Explanation: Best practices suggest that live response should follow the order of volatility, which means that you want to collect data which is changing the most rapidly. The order of volatility is: Memory Swap or page file Network status and current / recent network connections Running processes Open files

QUESTION 2

To detect worms and viruses buried deep within a network packet payload, Gigabytes worth of traffic content entering and exiting a network must be checked with which of the following technologies?

A. Proxy matching

B. Signature matching

C. Packet matching

D. Irregular expression matching

E. Object matching

Correct Answer: C

QUESTION 3

When an IDS system looks for a pattern indicating a known worm, what type of detection method is it using?

A. Signature-based

B. Anomaly-based

C. Statistical

D. Monitored

Correct Answer: A

QUESTION 4

What would a penetration tester expect to access after the following metasploit payload is delivered successfully?

Set PAYLOAD windows / shell / reverse _ tcp

A. VNC server session on the target

B. A netcat listener on the target

C. A meterpreter prompt on the target

D. A command prompt on the target

Correct Answer: D

Explanation: set PAYLOAD windows/shell/reverse_tcp should get you to a command prompt on the host system. A different payload is used to get a meterpreter session. This payload does not start a VNC server or netcat listener on the target system.

QUESTION 5

Which tasks would a First Responder perform during the Identification phase of Incident Response?

A. Verify the root cause of the incident and apply any missing security patches.

B. Install or reenable host-based firewalls and anti-virus software on suspected systems.

C. Search for sources of data and information that may be valuable in confirming and containing an incident.

D. Disconnect network communications and search for malicious executables or processes.

Correct Answer: C