GCED Q&As

GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

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

QUESTION 1

An incident response team is handling a worm infection among their user workstations. They created an

IPS signature to detect and block worm activity on the border IPS, then removed the worm\\'s artifacts or

workstations triggering the rule.

Despite this action, worm activity continued for days after. Where did the incident response team fail?

A. The team did not adequately apply lessons learned from the incident

B. The custom rule did not detect all infected workstations

C. They did not receive timely notification of the security event

D. The team did not understand the worm\\'s propagation method

Correct Answer: B

Explanation: Identifying and scoping an incident during triage is important to successfully handling a security incident. The detection methods used by the team didn\\'t detect all the infected workstations.

QUESTION 2

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 3

What piece of information would be recorded by the first responder as part of the initial System Description?

A. Copies of log files

B. System serial number

C. List of system directories

D. Hash of each hard drive

Correct Answer: B

QUESTION 4

Which tool uses a Snort rules file for input and by design triggers Snort alerts?

A. snot

B. stick

C. Nidsbench

D. ftester

Correct Answer: C

QUESTION 5

How does the Cisco IOS IP Source Guard feature help prevent spoofing attacks?

A. Filters traffic based on IP address once a DHCP address has been assigned

B. Prevents unauthorized MAC addresses from receiving an IP address on the network

C. Blocks unsolicited ARP packets after a client has received an IP address

D. Rate limits client traffic to prevent CAM table flooding

Correct Answer: A