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.leads4pass.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

Which Unix administration tool is designed to monitor configuration changes to Cisco, Extreme and Foundry infrastructure devices?

A. SNMP

B. Netflow

C. RANCID

D. RMON

Correct Answer: C

Explanation: RANCID is a Unix tool which can be used to monitor changes to the following networked devices and more: IOS, CatOS, PIX, Juniper, Foundry, HP ProCurve, Extreme.

QUESTION 2

When attempting to collect data from a suspected system compromise, which of the following should generally be collected first?

A. The network connections and open ports

B. The contents of physical memory

C. The current routing table

D. A list of the running services

Correct Answer: B

QUESTION 3

An incident response team investigated a database breach, and determined it was likely the result of an internal user who had a default password in place. The password was changed. A week later, they discover another loss of database records. The database admin provides logs that indicate the attack came from the front-end web interface. Where did the incident response team fail?

A. They did not eradicate tools left behind by the attacker

B. They did not properly identify the source of the breach

C. They did not lock the account after changing the password

D. They did not patch the database server after the event

Correct Answer: D

QUESTION 4

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 5

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.