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.pass2lead.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which control would BEST help detect a potential insider threat?

A. Mandatory approval process for executive and administrative access requests.

B. Providing the same access to all employees and monitoring sensitive file access.

C. Multiple scheduled log reviews of all employee access levels throughout the year

D. Requiring more than one employee to be trained on each task or job duty.

Correct Answer: A

QUESTION 2

What feature of Wireshark allows the analysis of one HTTP conversation?

A. Follow UDP Stream

B. Follow TCP Stream

C. Conversation list > IPV4

D. Setting a display filter to `tcp\\'

Correct Answer: B

Explanation: Follow TCP Stream is a feature of Wireshark that allows the analysis of a single TCP conversation between two hosts over multiple packets. Filtering packets using tcp in the filter box will return all TCP packets, not grouping by a single TCP conversation. HTTP is TCP not UDP, so you cannot follow a HTTP stream over UDP.

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

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 5

Which statement below is the MOST accurate about insider threat controls?

A. Classification of information assets helps identify data to protect.

B. Security awareness programs have a minimal impact on reducing the insider threat.

C. Both detective and preventative controls prevent insider attacks.

D. Rotation of duties makes an insider threat more likely.

E. Separation of duties encourages one employee to control a great deal of information.

Correct Answer: A

A company needs to classify its information as a key step in valuing it and knowing where to focus its protection. Rotation of duties and separation of duties are both key elements in reducing the scope of information access and the ability to conceal malicious behavior. Separation of duties helps minimize "empire building" within a company, keeping one individual from controlling a great deal of information, reducing the insider threat. Security awareness programs can help other employees notice the signs of an insider attack and thus reduce the insider threat. Detection is a reactive method and only occurs after an attack occurs. Only preventative methods can stop or limit an attack.