GCED Q&As

GIAC Certified Enterprise Defender Practice Test

QUESTION 1

Which of the following is the best way to establish and verify the integrity of a file before copying it during an investigation?

A. Write down the file size of the file before and after copying and ensure they match

B. Ensure that the MAC times are identical before and after copying the file

C. Establish the chain of custody with the system description to prove it is the same image

D. Create hash of the file before and after copying the image verifying they are identical

Correct Answer: D

QUESTION 2

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 3

Which of the following is an outcome of the initial triage during incident response?

A. Removal of unnecessary accounts from compromised systems

B. Segmentation of the network to protect critical assets

C. Resetting registry keys that vary from the baseline configuration

D. Determining whether encryption is in use on in scope systems

Correct Answer: B

QUESTION 4

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 5

Which Windows tool would use the following command to view a process: process where name=\\'suspect_malware.exe\\'list statistics

A. TCPView

B. Tasklist

C. WMIC

D. Netstat

Correct Answer: C