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

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

QUESTION 1

Which of the following is an operational security control that is used as a prevention mechanism?

A. Labeling of assets

B. Heat detectors

C. Vibration alarms

D. Voltage regulators

Correct Answer: A

Explanation: The following are considered operational security prevention controls: Security gates, guards, and dogs; Heating, ventilation, and air conditioning (HVAC); Fire suppressant; Labeling of assets (classification and responsible agents); Off-site storage (recovery); Safes and locks. The other distractors are considered operational security detection controls.

QUESTION 2

What should happen before acquiring a bit-for-bit copy of suspect media during incident response?

A. Encrypt the original media to protect the data

B. Create a one-way hash of the original media

C. Decompress files on the original media

D. Decrypt the original media

Correct Answer: B

QUESTION 3

What is the most common read-only SNMP community string usually called?

A. private

B. mib

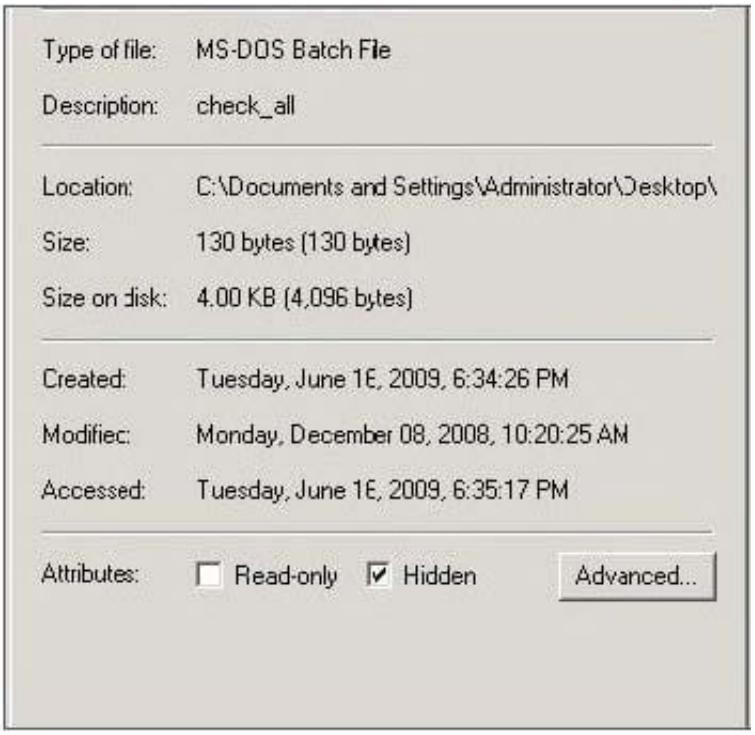
C. open

D. public

Correct Answer: D

QUESTION 4

Which command tool can be used to change the read-only or hidden setting of the file in the screenshot?



A. attrib

B. type

C. tasklist

D. dir

Correct Answer: A

Explanation: attrib ? or +r will remove or add the read only attribute from a file.

QUESTION 5

How does an Nmap connect scan work?

A. It sends a SYN, waits for a SYN/ACK, then sends a RST.

B. It sends a SYN, waits for a ACK, then sends a RST.

C. It sends a SYN, waits for a ACK, then sends a SYN/ACK.

D. It sends a SYN, waits for a SYN/ACK, then sends a ACK

Correct Answer: A

Explanation: An Nmap connect scan sends a SYN, waits for a SYN/ACK, then sends a ACK to complete the three-way handshake. A Nmap half-open scan sends a SYN, waits for a SYN/ACK, then sends a RST.

Latest GCED Dumps GCED PDF Dumps GCED Braindumps