GCED$^{\text{Q\&As}}$

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.pass4itsure.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 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 2

The creation of a filesystem timeline is associated with which objective?

A. Forensic analysis

B. First response

C. Access control

D. Incident eradication

Correct Answer: A

QUESTION 3

Why might an administrator not be able to delete a file using the Windows del command without specifying additional command line switches?

A. Because it has the read-only attribute set

B. Because it is encrypted

C. Because it has the nodel attribute set

D. Because it is an executable file

Correct Answer: A

QUESTION 4

A company wants to allow only company-issued devices to attach to the wired and wireless networks. Additionally, devices that are not up-to-date with OS patches need to be isolated from the rest of the network until they are updated. Which technology standards or protocols would meet these requirements?

A. 802.1x and Network Access Control

B. Kerberos and Network Access Control

C. LDAP and Authentication, Authorization and Accounting (AAA)

D. 802.11i and Authentication, Authorization and Accounting (AAA)

Correct Answer: A

QUESTION 5

Which tool keeps a backup of all deleted items, so that they can be restored later if need be?

A. ListDLLs

B. Yersinia

C. Ettercap

D. ProcessExplorer

E. Hijack This

Correct Answer: E

Explanation: After selecting "fix it!" with Hijack This you can always restore deleted items, because Hijack This keeps a backup of them.