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.passapply.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

What is needed to be able to use taskkill to end a process on remote system?

A. Svchost.exe running on the remote system

B. Domain login credentials

C. Port 445 open

D. Windows 7 or higher on both systems

Correct Answer: B

Explanation: Domain login credentials are needed to kill a process on a remote system using taskkill.

QUESTION 2

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 3

Which command is the Best choice for creating a forensic backup of a Linux system?

A. Run form a bootable CD: tar cvzf image.tgz /

B. Run from compromised operating system: tar cvzf image.tgz /

C. Run from compromised operating system: dd if=/ dev/hda1 of=/mnt/backup/hda1.img

D. Run from a bootable CD: dd if=/dev/hda1 of=/mnt/backup/hda1.img

Correct Answer: D

Explanation: Using dd from a bootable CD is the only forensically sound method of creating an image. Using tar does not capture slack space on the disk. Running any command from a compromised operating system will raise integrity issues.

QUESTION 4

Which of the following is a major problem that attackers often encounter when attempting to develop or use a kernel mode rootkit?

A. Their effectiveness depends on the specific applications used on the target system.

B. They tend to corrupt the kernel of the target system, causing it to crash.

C. They are unstable and are easy to identify after installation

D. They are highly dependent on the target OS.

Correct Answer: B

QUESTION 5

What would be the output of the following Google search? filetype:doc inurl:ws_ftp

A. Websites running ws_ftp that allow anonymous logins

B. Documents available on the ws_ftp.com domain

C. Websites hosting the ws_ftp installation program

D. Documents found on sites with ws_ftp in the web address

Correct Answer: D