GCED Q&As

GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

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

An outside vulnerability assessment reveals that users have been routinely accessing Gmail from work for over a year, a clear violation of this organization\\'s security policy. The users report "it just started working one day". Later, a network administrator admits he meant to unblock Gmail for just his own IP address, but he made a mistake in the firewall rule.

Which security control failed?

A. Access control

B. Authentication

C. Auditing

D. Rights management

Correct Answer: C

Explanation: Audits are used to identify irregular activity in logged (after-the-fact) records. If this activity went unnoticed or uncorrected for over a year, the internal audits failed because they were either incomplete or inaccurate. Authentication, access control and managing user rights would not apply as a network admin could be expected to have the ability to configure firewall rules.

QUESTION 3

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 4

At the start of an investigation on a Windows system, the lead handler executes the following commands after inserting a USB drive. What is the purpose of this command? C:\ >dir / s / a dhsra d: \ > a: \ IRCD.txt

A. To create a file on the USB drive that contains a listing of the C: drive

B. To show hidden and archived files on the C: drive and copy them to the USB drive

C. To copy a forensic image of the local C: drive onto the USB drive

D. To compare a list of known good hashes on the USB drive to files on the local C: drive

Correct Answer: C

Explanation: This command will create a text file on the collection media (in this case you would probably be using a USB flash drive) named IRCD.txt that should contain a recursive directory listing of all files on the desk.

QUESTION 5

An incident response team is handling a worm infection among their user workstations. They created an

IPS signature to detect and block worm activity on the border IPS, then removed the worm\\'s artifacts or

workstations triggering the rule.

Despite this action, worm activity continued for days after. Where did the incident response team fail?

A. The team did not adequately apply lessons learned from the incident

B. The custom rule did not detect all infected workstations

C. They did not receive timely notification of the security event

D. The team did not understand the worm\\'s propagation method

Correct Answer: B

Explanation: Identifying and scoping an incident during triage is important to successfully handling a security incident. The detection methods used by the team didn\\'t detect all the infected workstations.

GCED PDF Dumps GCED Study Guide GCED Exam Questions