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

QUESTION 1

An analyst wants to see a grouping of images that may be contained in a pcap file. Which tool natively meets this need?

A. Scapy

B. NetworkMiner

C. TCPReplay

D. Wireshark

Correct Answer: A

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

In order to determine if network traffic adheres to expected usage and complies with technical standards, an organization would use a device that provides which functionality?

A. Stateful packet filtering

B. Signature matching

C. Protocol anomaly detection

D. CRC checking

E. Forward error correction

Correct Answer: C

Explanation: In addition to standards compliance, Protocol Anomaly Detection determines whether data within the protocol adheres to expected usage. Even if a communication stream complies with a protocol standard, the way in which the protocol is being used may be inconsistent with what is expected. Perimeter devices that perform protocol anomaly detection contain in-depth knowledge of protocol standards and expected usage and are able to detect traffic that does not comply with those guidelines.

QUESTION 4

On which layer of the OSI Reference Model does the FWSnort utility function?

A. Physical Layer

B. Data Link Layer

C. Transport Layer

D. Session Layer

E. Application Layer

Correct Answer: C

Explanation: The FWSnort utility functions as a transport layer inline IPS.

QUESTION 5

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