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.pass2lead.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 SNMPv3 security feature that was not provided by earlier versions of the protocol?

A. Authentication based on RSA key pairs

B. The ability to change default community strings

C. AES encryption for SNMP network traffic

D. The ability to send SNMP traffic over TCP ports

Correct Answer: C

QUESTION 2

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 3

A company estimates a loss of $2,374 per hour in sales if their website goes down. Their webserver hosting site\\'s documented downtime was 7 hours each quarter over the last two years. Using the information, what can the analyst determine?

A. Annualized loss expectancy

B. CVSS risk score

C. Total cost of ownership

D. Qualitative risk posture

Correct Answer: A

Explanation: The annualized loss expectancy (ALE) is deduced by multiplying the single loss expectancy (SLE) by the annual rate of occurrence (ARO); in this example $2, 374 ?(7 ?4), respectively. This is a form of Quantitative risk analysis. Qualitative risk posture is deduced by measuring and contrasting the likelihood (probability of occurrence) with the level of impact and by definition does not address risk using monetary figures. Total cost of ownership (TCO) is the sum of all costs (technical, administrative, environmental, et al) that are involved for a specific system, service, etc. CVSS risk scoring is not based off of this type of loss data.

QUESTION 4

Which Windows CLI tool can identify the command-line options being passed to a program at startup?

A. netstat

B. attrib

C. WMIC

D. Tasklist

Correct Answer: C

QUESTION 5

Which Unix administration tool is designed to monitor configuration changes to Cisco, Extreme and Foundry infrastructure devices?

A. SNMP

B. Netflow

C. RANCID

D. RMON

Correct Answer: C

Explanation: RANCID is a Unix tool which can be used to monitor changes to the following networked devices and more: IOS, CatOS, PIX, Juniper, Foundry, HP ProCurve, Extreme.