312-39Q&As

Certified SOC Analyst (CSA)

Pass EC-COUNCIL 312-39 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/312-39.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL 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 technique involves scanning the headers of IP packets leaving a network to make sure that the unauthorized or malicious traffic never leaves the internal network?

A. Egress Filtering

B. Throttling

C. Rate Limiting

D. Ingress Filtering

Correct Answer: A

Reference: https://grokdesigns.com/wp-content/uploads/2018/04/CEH-v9-Notes.pdf (99)

QUESTION 2

Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:

http://www.terabytes.com/process.php./../../../../etc/passwd

A. Directory Traversal Attack

B. SQL Injection Attack

C. Denial-of-Service Attack

D. Form Tampering Attack

Correct Answer: B

Reference: https://doc.lagout.org/security/SQL%20Injection%20Attacks%20and%20Defense.pdf

QUESTION 3

What does Windows event ID 4740 indicate?

A. A user account was locked out.

B. A user account was disabled.

C. A user account was enabled.

D. A user account was created.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/windows/security/threat-

protection/auditing/event-4740#:~:text=For%204740(S)%3A%20A,Security%20ID"%20is%20not%20SYSTEM.

QUESTION 4

Which of the following is a report writing tool that will help incident handlers to generate efficient reports on detected incidents during incident response process?

A. threat_note

B. MagicTree

C. IntelMQ

D. Malstrom

Correct Answer: C

QUESTION 5

Which of the following is a default directory in a Mac OS X that stores security-related logs?

A. /private/var/log

B. /Library/Logs/Sync

C. /var/log/cups/access_log

D. ~/Library/Logs

Correct Answer: D