



312-39^{Q&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.geekcert.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

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 2

Which of the following technique protects from flooding attacks originated from the valid prefixes (IP addresses) so that they can be traced to its true source?

- A. Rate Limiting
- B. Egress Filtering
- C. Ingress Filtering
- D. Throttling

Correct Answer: C

Reference: <http://www.mecs-press.org/ijcnis/ijcnis-v5-n5/IJCNIS-V5-N5-6.pdf> (3)

QUESTION 3

Which of the following Windows Event Id will help you monitors file sharing across the network?

- A. 7045
- B. 4625
- C. 5140
- D. 4624

Correct Answer: C

Reference: <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5140>



QUESTION 4

Which of the following threat intelligence is used by a SIEM for supplying the analysts with context and "situational awareness" by using threat actor TTPs, malware campaigns, tools used by threat actors.

1.

Strategic threat intelligence

2.

Tactical threat intelligence

3.

Operational threat intelligence

4.

Technical threat intelligence

A. 2 and 3

B. 1 and 3

C. 3 and 4

D. 1 and 2

Correct Answer: A

Reference: <https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf> (38)

QUESTION 5

Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.

A. Dictionary Attack

B. Rainbow Table Attack

C. Bruteforce Attack

D. Syllable Attack

Correct Answer: A

Reference:

<https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic7-final/report.pdf>



VCE & PDF

GeekCert.com

<https://www.geekcert.com/312-39.html>

2024 Latest geekcert 312-39 PDF and VCE dumps Download

[Latest 312-39 Dumps](#)

[312-39 Study Guide](#)

[312-39 Braindumps](#)