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

Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

A. Hybrid Attack

B. Bruteforce Attack

C. Rainbow Table Attack

D. Birthday Attack

Correct Answer: B

Reference: https://www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/

QUESTION 2

Which of the following attack can be eradicated by using a safe API to avoid the use of the interpreter entirely?

A. Command Injection Attacks

B. SQL Injection Attacks

C. File Injection Attacks

D. LDAP Injection Attacks

Correct Answer: B

Reference: https://www.kiuwan.com/owasp-top-10-a1-injection/

QUESTION 3

In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

A. Evidence Gathering

B. Evidence Handling

C. Eradication

D. Systems Recovery

Correct Answer: A

Reference: https://www.eccouncil.org/wp-content/uploads/2019/02/ECIH-V2-Brochure.pdf

QUESTION 4

Which of the following is a Threat Intelligence Platform?

A. SolarWinds MS

B. TC Complete

C. Keepnote

D. Apility.io

Correct Answer: A

Reference: https://www.esecurityplanet.com/products/threat-intelligence-platforms/

QUESTION 5

Which of the following attacks causes sudden changes in file extensions or increase in file renames at rapid speed?

A. Ransomware Attack

B. DoS Attack

C. DHCP starvation Attack

D. File Injection Attack

Correct Answer: A

Reference: https://www.netfort.com/category/ransomware-detection/

[Latest 312-39 Dumps](#)   [312-39 PDF Dumps](#)   [312-39 Practice Test](#)