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.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

QUESTION 1

An attacker exploits the logic validation mechanisms of an e-commerce website. He successfully purchases a product worth $100 for $10 by modifying the URL exchanged between the client and the server.

Original URL: http://www.buyonline.com/product.aspx?profile=12anddebit=100 Modified URL: http://www.buyonline.com/product.aspx?profile=12anddebit=10 Identify the attack depicted in the above scenario.

A. Denial-of-Service Attack

B. SQL Injection Attack

C. Parameter Tampering Attack

D. Session Fixation Attack

Correct Answer: D

QUESTION 2

Which of the following attack can be eradicated by disabling of "allow_url_fopen and allow_url_include" in the php.ini file?

A. File Injection Attacks

B. URL Injection Attacks

C. LDAP Injection Attacks

D. Command Injection Attacks

Correct Answer: B

QUESTION 3

Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?

A. Rule-based detection

B. Heuristic-based detection

C. Anomaly-based detection

D. Signature-based detection

Correct Answer: C

QUESTION 4

Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?

A. /etc/ossim/reputation

B. /etc/ossim/siem/server/reputation/data

C. /etc/siem/ossim/server/reputation.data

D. /etc/ossim/server/reputation.data

Correct Answer: A

QUESTION 5

John as a SOC analyst is worried about the amount of Tor traffic hitting the network. He wants to prepare a dashboard in the SIEM to get a graph to identify the locations from where the TOR traffic is coming. Which of the following data source will he use to prepare the dashboard?

A. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.

B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.

C. DNS/ Web Server logs with IP addresses.

D. Apache/ Web Server logs with IP addresses and Host Name.

Correct Answer: D