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.certbus.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

What is the process of monitoring and capturing all data packets passing through a given network using different tools?

A. Network Scanning

B. DNS Footprinting

C. Network Sniffing

D. Port Scanning

Correct Answer: C

Reference: https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types

QUESTION 2

What does HTTPS Status code 403 represents?

A. Unauthorized Error

B. Not Found Error

C. Internal Server Error

D. Forbidden Error

Correct Answer: D

Reference: https://en.wikipedia.org/wiki/HTTP_403

QUESTION 3

Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

A. Windows Event Log

B. Web Server Logs

C. Router Logs

D. Switch Logs

Correct Answer: B

QUESTION 4

According to the Risk Matrix table, what will be the risk level when the probability of an attack is very low and the impact

of that attack is major?

A. High

B. Extreme

C. Low

D. Medium

Correct Answer: C

Reference: https://www.moheri.gov.om/userupload/Policy/IT%20Risk%20Management%20Framework.pdf (17)

QUESTION 5

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 6

Which one of the following is the correct flow for Setting Up a Computer Forensics Lab?

A. Planning and budgeting

Correct Answer: A

Reference: https://info-savvy.com/setting-up-a-computer-forensics-lab/

QUESTION 7

What does the HTTP status codes 1XX represents?

A. Informational message

B. Client error

C. Success

D. Redirection

Correct Answer: A

Reference: https://en.wikipedia.org/wiki/List_of_HTTP_status_codes#:~:text=1xx%20informational%20response%20?20the%20request,syntax%20or%20cannot%20be%20fulfilled

QUESTION 8

John, a SOC analyst, while monitoring and analyzing Apache web server logs, identified an event log matching Regex /(\.|(%|%25)2E)(\.|(%|%25)2E)(\/|(%|%25)2F|\\|(%|%25)5C)/i. What does this event log indicate?

A. XSS Attack

B. SQL injection Attack

C. Directory Traversal Attack

D. Parameter Tampering Attack

Correct Answer: A

QUESTION 9

Banter is a threat analyst in Christine Group of Industries. As a part of the job, he is currently formatting and structuring the raw data. He is at which stage of the threat intelligence life cycle?

A. Dissemination and Integration

B. Processing and Exploitation

C. Collection

D. Analysis and Production

Correct Answer: B

Reference: https://socradar.io/5-stages-of-the-threat-intelligence-lifecycle/

QUESTION 10

Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.

Identify the stage in which he is currently in.

A. Post-Incident Activities

B. Incident Recording and Assignment

C. Incident Triage

D. Incident Disclosure

Correct Answer: B

QUESTION 11

Which encoding replaces unusual ASCII characters with "%" followed by the character\\'s two-digit ASCII code expressed in hexadecimal?

A. Unicode Encoding

B. UTF Encoding

C. Base64 Encoding

D. URL Encoding

Correct Answer: D

Reference: https://ktflash.gitbooks.io/ceh_v9/content/125_countermeasures.html

QUESTION 12

A type of threat intelligent that find out the information about the attacker by misleading them is known as _____.

A. Threat trending Intelligence

B. Detection Threat Intelligence

C. Operational Intelligence

D. Counter Intelligence

Correct Answer: C

Reference: https://www.recordedfuture.com/threat-intelligence/

QUESTION 13

Which of the following steps of incident handling and response process focus on limiting the scope and extent of an incident?

A. Containment

B. Data Collection

C. Eradication

D. Identification

Correct Answer: A

QUESTION 14

In which phase of Lockheed Martin\\'s

Correct Answer: B

Reference: https://securityboulevard.com/2018/08/the-cyber-kill-chain-what-you-need-to-know/

QUESTION 15

Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex /((\%3C)|)/|. What does this event log indicate?

A. Directory Traversal Attack

B. Parameter Tampering Attack

C. XSS Attack

D. SQL Injection Attack

Correct Answer: C

Reference: https://books.google.com.pk/books?id=PDR4nOAP8qUCandpg=PA87andlpg=PA87anddq=regex+/((%5C%253C)%7C)/% 7Candsource=blandots=kOBHNfJmtqandsig=ACfU3U2CG_hELc1HMb1chdc9OS4ooXPlMgandhl=enandsa=Xandved=2ahUKEwjYwJmlt_buAhUFShUIHTBNAs8Q6AEwBXoECAUQAw#v=onepageandqandf=false