EC-COUNCIL.312-39.v2022-02-17.q36

Exam Code:	312-39
Exam Name:	Certified SOC Analyst (CSA)
Certification Provider:	EC-COUNCIL
Free Question Number:	36
Version:	v2022-02-17
# of views:	873
# of Questions views:	360
https://www.dumpsdb.com/dumps/EC-COUNCIL/312-39/EC-COUNCIL.312-39.v2022-02-17.q36	

NEW QUESTION: 1
Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As a part of threat intelligent strategy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in.
Which one of the following components he should include in the above threat intelligent strategy plan to make it effective?
A. Threat trending
B. Threat buy-in
C. Threat pivoting
D. Threat boosting
Answer: (SHOW ANSWER)

NEW QUESTION: 2
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. Birthday Attack
C. Rainbow Table Attack
D. Bruteforce Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 3

Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex /\\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix.
What does this event log indicate?
A. XSS Attack
B. SQL Injection Attack
C. Directory Traversal Attack
D. Parameter Tampering Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?
A. Preparation -> Incident Recording -> Incident Triage -> Containment -> Eradication -> Recovery -> Post-Incident Activities
B. Incident Triage -> Eradication -> Containment -> Incident Recording -> Preparation -> Recovery -> Post-Incident Activities
C. Incident Recording -> Preparation -> Containment -> Incident Triage -> Recovery -> Eradication -> Post-Incident Activities
D. Containment -> Incident Recording -> Incident Triage -> Preparation -> Recovery -> Eradication -> Post-Incident Activities
Answer: A (LEAVE A REPLY)

NEW QUESTION: 5
Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.
A. Syllable Attack
B. Dictionary Attack
C. Bruteforce Attack
D. Rainbow Table Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
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

Answer: (SHOW ANSWER)

NEW QUESTION: 7
John, a threat analyst at GreenTech Solutions, wants to gather information about specific threats against the organization. He started collecting information from various sources, such as humans, social media, chat room, and so on, and created a report that contains malicious activity.
Which of the following types of threat intelligence did he use?
A. Operational Threat Intelligence
B. Technical Threat Intelligence
C. Tactical Threat Intelligence
D. Strategic Threat Intelligence
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
Which of the following tool can be used to filter web requests associated with the SQL Injection attack?
A. Nmap
B. UrlScan
C. Hydra
D. ZAP proxy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 9
Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.
A. Reconnaissance Attack
B. Ransomware Attack
C. DoS Attack
D. Man-In-Middle Attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
Which of the following attack can be eradicated by filtering improper XML syntax?
A. Web Services Attacks
B. CAPTCHA Attacks
C. Insufficient Logging and Monitoring Attacks
D. SQL Injection Attacks
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11

Which of the following framework describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering?

A. SSE-CMM

B. COBIT

C. ITIL

D. SOC-CMM

Answer: A (LEAVE A REPLY)

NEW QUESTION: 12

Which of the following formula represents the risk?

A. Risk = Likelihood * Consequence * Severity

B. Risk = Likelihood * Impact * Asset Value

C. Risk = Likelihood * Severity * Asset Value

D. Risk = Likelihood * Impact * Severity

Answer: (SHOW ANSWER)

NEW QUESTION: 13

Which of the following tool is used to recover from web application incident?

A. Proxy Workbench

B. CrowdStrike FalconTM Orchestrator

C. Smoothwall SWG

D. Symantec Secure Web Gateway

Answer: (SHOW ANSWER)

NEW QUESTION: 14

Which of the following fields in Windows logs defines the type of event occurred, such as Correlation Hint, Response Time, SQM, WDI Context, and so on?

A. Level

B. Keywords

C. Source

D. Task Category

Answer: B (LEAVE A REPLY)

NEW QUESTION: 15

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. LDAP Injection Attacks

D. File Injection Attacks

Answer: B (LEAVE A REPLY)

NEW QUESTION: 16
Which of the following attack can be eradicated by converting all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums?
A. XSS Attacks
B. Session Management Attacks
C. Web Services Attacks
D. Broken Access Control Attacks
Answer: A (LEAVE A REPLY)

Valid 312-39 Dumps shared by TrainingQuiz.com for Helping Passing 312-39 Exam! TrainingQuiz.com now offer the **newest 312-39 exam dumps**, the TrainingQuiz.com 312-39 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 312-39 dumps with Test Engine here: https://www.trainingquiz.com/312-39-practice-quiz.html (**102** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 17
In which phase of Lockheed Martin's - Cyber Kill Chain Methodology, adversary creates a deliverable malicious payload using an exploit and a backdoor?
A. Delivery
B. Reconnaissance
C. Exploitation
D. Weaponization
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which of the following is a Threat Intelligence Platform?
A. Apility.io
B. TC Complete
C. Keepnote
D. SolarWinds MS
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 20
An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted code at the end of the company's URL as follows:
http://technosoft.com.com/<script>alert("WARNING: The application has encountered an error");</script>.
Identify the attack demonstrated in the above scenario.
A. SQL Injection Attack
B. Session Attack
C. Denial-of-Service Attack
D. Cross-site Scripting Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21
Jason, a SOC Analyst with Maximus Tech, was investigating Cisco ASA Firewall logs and came across the following log entry:
May 06 2018 21:27:27 asa 1: %ASA -5 - 11008: User 'enable_15' executed the 'configure term' command What does the security level in the above log indicates?
A. Normal but significant message
B. Informational message
C. Critical condition message
D. Warning condition message
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22
Which of the following are the responsibilities of SIEM Agents?
1.Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.
2.Normalizing data received from various devices sending data to SIEM before forwarding it to the central engine.
3.Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.
4.Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.
A. 3 and 1
B. 1 and 4
C. 1 and 2
D. 2 and 3
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
Daniel is a member of an IRT, which was started recently in a company named Mesh Tech. He wanted to find the purpose and scope of the planned incident response capabilities.
What is he looking for?
A. Incident Response Mission
B. Incident Response Resources
C. Incident Response Vision
D. Incident Response Intelligence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
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. Form Tampering Attack
B. Directory Traversal Attack
C. Denial-of-Service Attack
D. SQL Injection Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following Windows Event Id will help you monitors file sharing across the network?
A. 4625
B. 5140
C. 4624
D. 7045
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
Which of the following Windows event is logged every time when a user tries to access the "Registry" key?
A. 4656
B. 4663
C. 4657
D. 4660
Answer: (SHOW ANSWER)

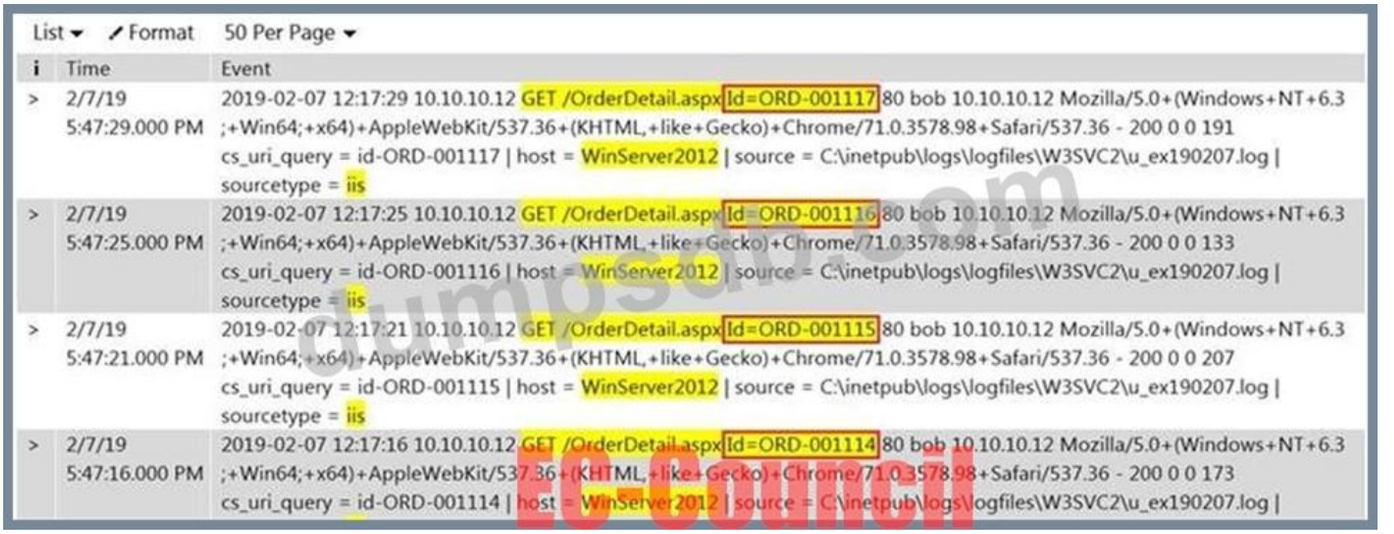
NEW QUESTION: 27
Identify the HTTP status codes that represents the server error.
A. 2XX
B. 5XX

C. 1XX
D. 4XX
Answer: (SHOW ANSWER)

NEW QUESTION: 28
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. Low
B. High
C. Extreme
D. Medium
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
What type of event is recorded when an application driver loads successfully in Windows?
A. Success Audit
B. Error
C. Warning
D. Information
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.



What does this event log indicate?
A. Parameter Tampering Attack
B. XSS Attack
C. SQL Injection Attack
D. Directory Traversal Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Properly applied cyber threat intelligence to the SOC team help them in discovering TTPs.
What does these TTPs refer to?
A. Tactics, Targets, and Process
B. Tactics, Threats, and Procedures
C. Tactics, Techniques, and Procedures
D. Targets, Threats, and Process
Answer: C (LEAVE A REPLY)

Valid 312-39 Dumps shared by TrainingQuiz.com for Helping Passing 312-39 Exam! TrainingQuiz.com now offer the **newest 312-39 exam dumps**, the TrainingQuiz.com 312-39 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 312-39 dumps with Test Engine here: https://www.trainingquiz.com/312-39-practice-quiz.html (**102** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 32
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=12
&debit=100
Modified URL: http://www.buyonline.com/product.aspx?profile=12
&debit=10
Identify the attack depicted in the above scenario.
A. SQL Injection Attack
B. Denial-of-Service Attack
C. Session Fixation Attack
D. Parameter Tampering Attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
Which of the following process refers to the discarding of the packets at the routing level without informing the source that the data did not reach its intended recipient?
A. Drop Requests
B. Rate Limiting
C. Black Hole Filtering
D. Load Balancing
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Which of the following threat intelligence helps cyber security professionals such as security operations managers, network operations center and incident responders to understand how the adversaries are expected to perform the attack on the organization, and the technical capabilities and goals of the attackers along with the attack vectors?
A. Operational Threat Intelligence
B. Tactical Threat Intelligence
C. Analytical Threat Intelligence
D. Strategic Threat Intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 35
In which log collection mechanism, the system or application sends log records either on the local disk or over the network.
A. pull-based
B. rule-based
C. push-based
D. signature-based
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.
A. Error
B. Warning
C. Information
D. Failure Audit
Answer: (SHOW ANSWER)

Valid 312-39 Dumps shared by TrainingQuiz.com for Helping Passing 312-39 Exam! TrainingQuiz.com now offer the **newest 312-39 exam dumps**, the TrainingQuiz.com 312-39 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 312-39 dumps with Test Engine here: https://www.trainingquiz.com/312-39-practice-quiz.html (**102** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)