

EC-COUNCIL.312-39.v2021-11-15.q35

Exam Code:	312-39
Exam Name:	Certified SOC Analyst (CSA)
Certification Provider:	EC-COUNCIL
Free Question Number:	35
Version:	v2021-11-15
# of views:	1335
# of Questions views:	350
https://www.freepdfdumps.com/EC-COUNCIL.312-39.v2021-11-15.q35.html	

NEW 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=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. Parameter Tampering Attack
- C. Denial-of-Service Attack
- D. Session Fixation Attack

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 2

Which of the following stage executed after identifying the required event sources?

- A. Implementing and Testing the Use Case
- B. Defining Rule for the Use Case
- C. Identifying the monitoring Requirements
- D. Validating the event source against monitoring requirement

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 3

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 Intelligence
- B. Incident Response Mission
- C. Incident Response Vision
- D. Incident Response Resources

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 4

Which of the following tool can be used to filter web requests associated with the SQL Injection attack?

- A. UrlScan
- B. ZAP proxy
- C. Hydra
- D. Nmap

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 5

Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.

- A. Man-In-Middle Attack
- B. DoS Attack
- C. Ransomware Attack
- D. Reconnaissance Attack

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 6

Properly applied cyber threat intelligence to the SOC team help them in discovering TTPs.

What does these TTPs refer to?

- A. Tactics, Techniques, and Procedures
- B. Targets, Threats, and Process
- C. Tactics, Threats, and Procedures
- D. Tactics, Targets, and Process

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

Which of the following Windows features is used to enable Security Auditing in Windows?

- A. Windows Defender
- B. Windows Firewall
- C. Bitlocker
- D. Local Group Policy Editor

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 8

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

- A. Counter Intelligence
- B. Operational Intelligence
- C. Detection Threat Intelligence
- D. Threat trending Intelligence

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 9

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: ([SHOW ANSWER](#))

NEW QUESTION: 10

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

- A. Port Scanning
- B. DNS Footprinting
- C. Network Sniffing
- D. Network Scanning

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 11

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. Session Management Attacks
- B. XSS Attacks
- C. Broken Access Control Attacks
- D. Web Services Attacks

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 12

What is the correct sequence of SOC Workflow?

- A. Collect, Ingest, Validate, Report, Respond, Document
- B. Collect, Ingest, Document, Validate, Report, Respond
- C. Collect, Respond, Validate, Ingest, Report, Document
- D. Collect, Ingest, Validate, Document, Report, Respond

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 13

What does Windows event ID 4740 indicate?

- A. A user account was enabled.
- B. A user account was disabled.
- C. A user account was locked out.
- D. A user account was created.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 14

Identify the attack in which the attacker exploits a target system through publicly known but still unpatched vulnerabilities.

- A. DHCP Starvation
- B. Zero-Day Attack
- C. Slow DoS Attack
- D. DNS Poisoning Attack

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 15

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. Cross-site Scripting Attack
- C. Session Attack
- D. Denial-of-Service Attack

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 16

Bonney's system has been compromised by a gruesome malware.

What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?

- A. Call the legal department in the organization and inform about the incident
- B. Turn off the infected machine
- C. Leave it to the network administrators to handle
- D. Complaint to police in a formal way regarding the incident

Answer: B ([LEAVE A REPLY](#))

Valid 312-39 Dumps shared by Actual4test.com for Helping Passing 312-39 Exam! Actual4test.com now offer the **newest 312-39 exam dumps**, the Actual4test.com 312-39 exam **questions have been updated** and **answers have been corrected** get the

NEW QUESTION: 17

Which of the following formula is used to calculate the EPS of the organization?

- A. $\text{EPS} = \text{average number of correlated events} / \text{time in seconds}$
- B. $\text{EPS} = \text{number of normalized events} / \text{time in seconds}$
- C. $\text{EPS} = \text{number of security events} / \text{time in seconds}$
- D. $\text{EPS} = \text{number of correlated events} / \text{time in seconds}$

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 18

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

- A. UTF Encoding
- B. Base64 Encoding
- C. Unicode Encoding
- D. URL Encoding

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 19

Which of the following attack can be eradicated by filtering improper XML syntax?

- A. SQL Injection Attacks
- B. Web Services Attacks
- C. CAPTCHA Attacks
- D. Insufficient Logging and Monitoring Attacks

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 20

Which of the following can help you eliminate the burden of investigating false positives?

- A. Ingesting the context data
- B. Treating every alert as high level
- C. Keeping default rules
- D. Not trusting the security devices

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 21

Jony, a security analyst, while monitoring IIS logs, identified events shown in the figure below.

_time	cs_uri_query
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+WAITFOR DELAY '0:0:5'--
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+WAITFOR DELAY '0:0:5'--
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+WAITFOR DELAY '0:0:5'--

What does this event log indicate?

- A. Parameter Tampering Attack
- B. XSS Attack
- C. SQL Injection Attack
- D. Directory Traversal Attack

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 22

Which of the following factors determine the choice of SIEM architecture?

- A. SMTP Configuration
- B. Network Topology
- C. DHCP Configuration
- D. DNS Configuration

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 23

The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk.

What kind of threat intelligence described above?

- A. Functional Threat Intelligence
- B. Tactical Threat Intelligence
- C. Operational Threat Intelligence
- D. Strategic Threat Intelligence

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 24

Which of the following Windows event is logged every time when a user tries to access the "Registry" key?

- A. 4660
- B. 4657
- C. 4656
- D. 4663

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 25

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. Black Hole Filtering
- B. Drop Requests
- C. Load Balancing
- D. Rate Limiting

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 26

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. Rainbow Table Attack
- B. Hybrid Attack
- C. Bruteforce Attack
- D. Birthday Attack

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 27

Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?

- A. DARPA
- B. PCI-DSS
- C. HIPAA
- D. FISMA

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 28

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

- A. Rainbow Table Attack
- B. Bruteforce Attack
- C. Syllable Attack
- D. Dictionary Attack

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 29

Which of the following formula represents the risk levels?

- A. Level of risk = Consequence * Asset Value
- B. Level of risk = Consequence * Impact

C. Level of risk = Consequence * Likelihood

D. Level of risk = Consequence * Severity

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 30

An organization is implementing and deploying the SIEM with following capabilities.



What kind of SIEM deployment architecture the organization is planning to implement?

A. Self-hosted, Jointly Managed

B. Cloud, MSSP Managed

C. Self-hosted, MSSP Managed

D. Self-hosted, Self-Managed

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 31

Ray is a SOC analyst in a company named Queens Tech. One Day, Queens Tech is affected by a DoS/DDoS attack. For the containment of this incident, Ray and his team are trying to provide additional bandwidth to the network devices and increasing the capacity of the servers.

What is Ray and his team doing?

A. Blocking the Attacks

B. Absorbing the Attack

C. Diverting the Traffic

D. Degrading the services

Answer: ([SHOW ANSWER](#))

Valid 312-39 Dumps shared by Actual4test.com for Helping Passing 312-39 Exam! Actual4test.com now offer the **newest 312-39 exam dumps**, the Actual4test.com 312-39 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 312-39 dumps with Test Engine here: https://www.actual4test.com/312-39_examcollection.html (202 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 32

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

List ▾ / Format 50 Per Page ▾		
i	Time	Event
>	2/7/19 5:47:29.000 PM	2019-02-07 12:17:29 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001117 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 191 cs_uri_query = id-ORD-001117 host = WinServer2012 source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log sourcetype = iis
>	2/7/19 5:47:25.000 PM	2019-02-07 12:17:25 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001116 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 133 cs_uri_query = id-ORD-001116 host = WinServer2012 source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log sourcetype = iis
>	2/7/19 5:47:21.000 PM	2019-02-07 12:17:21 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001115 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 207 cs_uri_query = id-ORD-001115 host = WinServer2012 source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log sourcetype = iis
>	2/7/19 5:47:16.000 PM	2019-02-07 12:17:16 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001114 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 173 cs_uri_query = id-ORD-001114 host = WinServer2012 source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log

What does this event log indicate?

- A. Directory Traversal Attack
- B. XSS Attack
- C. Parameter Tampering Attack
- D. SQL Injection Attack

Answer: C (LEAVE A REPLY)

NEW QUESTION: 33

An organization wants to implement a SIEM deployment architecture. However, they have the capability to do only log collection and the rest of the SIEM functions must be managed by an MSSP.

Which SIEM deployment architecture will the organization adopt?

- A. Cloud, MSSP Managed
- B. Self-hosted, Self-Managed
- C. Self-hosted, MSSP Managed
- D. Self-hosted, Jointly Managed

Answer: C (LEAVE A REPLY)

NEW QUESTION: 34

If the SIEM generates the following four alerts at the same time:

- I.Firewall blocking traffic from getting into the network alerts
- II.SQL injection attempt alerts

III.Data deletion attempt alerts

IV.Brute-force attempt alerts

Which alert should be given least priority as per effective alert triaging?

A. III

B. I

C. II

D. IV

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 35

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

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

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

D. DNS/ Web Server logs with IP addresses.

Answer: C ([LEAVE A REPLY](#))

Valid 312-39 Dumps shared by Actual4test.com for Helping Passing 312-39 Exam! Actual4test.com now offer the **newest 312-39 exam dumps**, the Actual4test.com 312-39 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 312-39 dumps with Test Engine here: https://www.actual4test.com/312-39_examcollection.html (202 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)