

EC-Council

Exam Questions 312-39

Certified SOC Analyst (CSA)



NEW QUESTION 1

Which of the following is a default directory in a Mac OS X that stores security-related logs?

- A. /private/var/log
- B. /Library/Logs/Sync
- C. /var/log/cups/access_log
- D. ~/Library/Logs

Answer: D

NEW QUESTION 2

What does the Security Log Event ID 4624 of Windows 10 indicate?

- A. Service added to the endpoint
- B. A share was assessed
- C. An account was successfully logged on
- D. New process executed

Answer: C

NEW QUESTION 3

Harley is working as a SOC analyst with Powell Tech. Powell Inc. is using Internet Information Service (IIS) version 7.0 to host their website. Where will Harley find the web server logs, if he wants to investigate them for any anomalies?

- A. SystemDrive%\inetpub\logs\LogFiles\W3SVCN
- B. SystemDrive%\LogFiles\inetpub\logs\W3SVCN
- C. %SystemDrive%\LogFiles\logs\W3SVCN
- D. SystemDrive%\ inetpub\LogFiles\logs\W3SVCN

Answer: B

NEW QUESTION 4

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

Answer: D

NEW QUESTION 5

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

Answer: C

NEW QUESTION 6

Which of the following formula represents the risk levels?

- A. Level of risk = Consequence × Severity
- B. Level of risk = Consequence × Impact
- C. Level of risk = Consequence × Likelihood
- D. Level of risk = Consequence × Asset Value

Answer: B

NEW QUESTION 7

Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?

- A. De-Militarized Zone (DMZ)
- B. Firewall
- C. Honeypot
- D. Intrusion Detection System

Answer: C

NEW QUESTION 8

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

Answer: B

NEW QUESTION 9

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 pivoting
- B. Threat trending
- C. Threat buy-in
- D. Threat boosting

Answer: C

NEW QUESTION 10

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

Answer: A

NEW QUESTION 10

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

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

Answer: D

NEW QUESTION 12

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

Answer: D

NEW QUESTION 16

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. Denial-of-Service Attack
- B. SQL Injection Attack
- C. Parameter Tampering Attack
- D. Session Fixation Attack

Answer: D

NEW QUESTION 20

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

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

Answer: B

NEW QUESTION 25

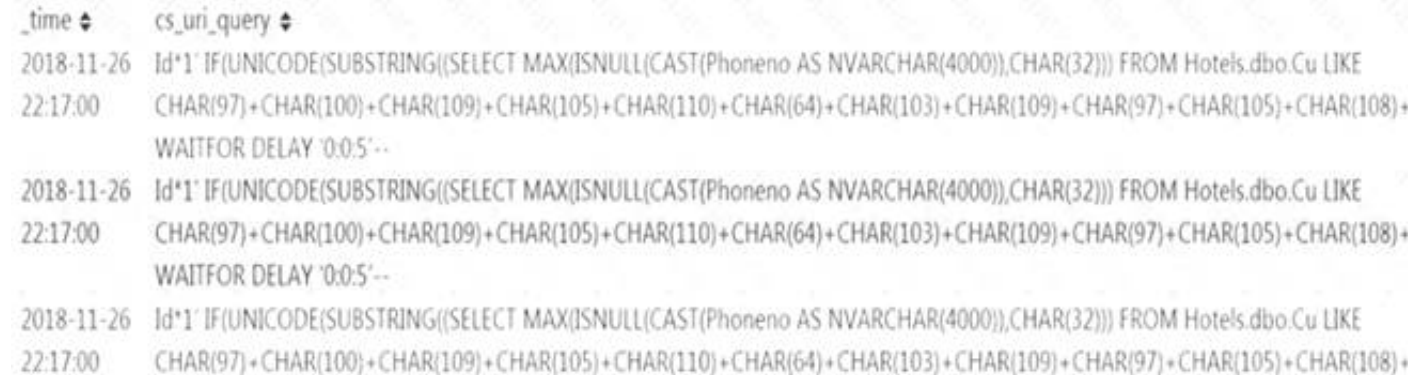
Which one of the following is the correct flow for Setting Up a Computer Forensics Lab?

- A. Planning and budgeting → Physical location and structural design considerations → Work area considerations → Human resource considerations → Physical security recommendations → Forensics lab licensing
- B. Planning and budgeting → Physical location and structural design considerations → Forensics lab licensing → Human resource considerations → Work area considerations → Physical security recommendations
- C. Planning and budgeting → Forensics lab licensing → Physical location and structural design considerations → Work area considerations → Physical security recommendations → Human resource considerations
- D. Planning and budgeting → Physical location and structural design considerations → Forensics lab licensing → Work area considerations → Human resource considerations → Physical security recommendations

Answer: A

NEW QUESTION 26

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)+
```

What does this event log indicate?

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

Answer: A

NEW QUESTION 27

Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?

- A. Netstat Data
- B. DNS Data
- C. IIS Data
- D. DHCP Data

Answer: A

NEW QUESTION 30

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

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

Answer: B

NEW QUESTION 31

Peter, a SOC analyst with Spade Systems, is monitoring and analyzing the router logs of the company and wanted to check the logs that are generated by access control list numbered 210.

What filter should Peter add to the 'show logging' command to get the required output?

- A. show logging | access 210
- B. show logging | forward 210
- C. show logging | include 210
- D. show logging | route 210

Answer: C

NEW QUESTION 36

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

Answer: C

NEW QUESTION 40

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

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

Answer: A

NEW QUESTION 44

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

NEW QUESTION 45

Which of the following is a Threat Intelligence Platform?

- A. SolarWinds MS
- B. TC Complete
- C. Keepnote
- D. Apility.io

Answer: A

NEW QUESTION 49

What type of event is recorded when an application driver loads successfully in Windows?

- A. Error
- B. Success Audit
- C. Warning
- D. Information

Answer: D

NEW QUESTION 53

In which log collection mechanism, the system or application sends log records either on the local disk or over the network.

- A. rule-based
- B. pull-based
- C. push-based
- D. signature-based

Answer: A

NEW QUESTION 58

Which of the log storage method arranges event logs in the form of a circular buffer?

- A. FIFO
- B. LIFO
- C. non-wrapping
- D. wrapping

Answer: A

NEW QUESTION 61

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

Answer: A

NEW QUESTION 65

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

Answer: B

NEW QUESTION 70

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

312-39 Practice Exam Features:

- * 312-39 Questions and Answers Updated Frequently
- * 312-39 Practice Questions Verified by Expert Senior Certified Staff
- * 312-39 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 312-39 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-39 Practice Test Here](#)