



Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.



312-39 Practice Questions
312-39 Practice Test
312-39 Practice Exam
312-39 Exam Questions
312-39 Study Guide



killexams.com

EC-Council

312-39

EC-Council Certified SOC Analyst (CSA) certification

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/312-39>



Question: 14

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: C

Question: 15

Chloe, a SOC analyst with Jake Tech, is checking Linux systems logs. She is investigating files at /var/log/wtmp.

What Chloe is looking at?

- A. Error log
- B. System boot log
- C. General message and system-related stuff
- D. Login records

Answer: D

Explanation:

Reference: <https://stackify.com/linux-logs/>

Question: 16

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

Answer: D

Question: 17

According to the forensics investigation process, what is the next step carried out right after collecting the evidence?

- A. Create a Chain of Custody Document
- B. Send it to the nearby police station
- C. Set a Forensic lab
- D. Call Organizational Disciplinary Team

Answer: A

Question: 18

Which of the following command is used to enable logging in iptables?

- A. \$ iptables -B INPUT -j LOG
- B. \$ iptables -A OUTPUT -j LOG
- C. \$ iptables -A INPUT -j LOG
- D. \$ iptables -B OUTPUT -j LOG

Answer: C

Question: 19

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

- C. Leave it to the network administrators to handle
- D. Call the legal department in the organization and inform about the incident

Answer: B

Question: 25

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: D

Explanation:

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

Question: 26

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

NOTE: It is mandatory to answer the question before proceeding to the next one.

- A. High
- B. Extreme
- C. Low
- D. Medium

Answer: B

Question: 27

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

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. SQL Injection Attack
- D. Parameter Tampering Attack

Answer: D

Explanation:

Reference: <https://infosecwriteups.com/what-is-parameter-tampering-5b1beb12c5ba>

Question: 28

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

Answer: B

Explanation:

Reference: <https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/threat-intelligence/what-is-threat-intelligence/>

Question: 29

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: C

Question: 30

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, Jointly Managed
- C. Self-hosted, MSSP Managed
- D. Self-hosted, Self-Managed

Answer: C

Question: 31

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

Answer: C

Explanation:

Reference: [https://en.wikipedia.org/wiki/Black_hole_\(networking\)#:~:text=In%20networking%2C%20black%20holes%20refer,not%20reach%20its%20intended%20recipient.](https://en.wikipedia.org/wiki/Black_hole_(networking)#:~:text=In%20networking%2C%20black%20holes%20refer,not%20reach%20its%20intended%20recipient.)

Question: 32

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

Question: 33

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

- A. CrowdStrike Falcon™ Orchestrator
- B. Symantec Secure Web Gateway
- C. Smoothwall SWG
- D. Proxy Workbench

Answer: A

Question: 34

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. Keywords
- B. Task Category
- C. Level
- D. Source

Answer: A

Question: 35

Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?

- A. `$ tailf /var/log/sys/kern.log`
- B. `$ tailf /var/log/kern.log`
- C. `# tailf /var/log/messages`
- D. `# tailf /var/log/sys/messages`

Answer: B

Explanation:

Reference: <https://tecadmin.net/enable-logging-in-iptables-on-linux/>

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllabus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.