Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

312-39 Dumps
312-39 Braindumps
312-39 Real Questions
312-39 Practice Test
312-39 Actual Questions

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

Answer: C

Question: 20

What does the HTTP status codes 1XX represents?

A. Informational message
B. Client error
C. Success
D. Redirection

Answer: A

Explanation:

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

Question: 21

Which of the following is a report writing tool that will help incident handlers to generate efficient reports on detected incidents during incident response process?

A. threat_note
B. MagicTree
C. IntelMQ
D. Malstrom

Answer: B

Question: 22

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. Diverting the Traffic
C. Degrading the services
D. Absorbing the Attack

Answer: D

Question: 23

Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex /\w*((%27)|(â))((%6F)|o|(%4F))((%72)|r|(%52))/ix.

What does this event log indicate?

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

Answer: A

Explanation:

Reference: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=001f5e09-88b4-4a9a-b310-4c20578eecf9&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Question: 24

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. Complaint to police in a formal way regarding the incident
B. Turn off the infected machine

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.

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.

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 FalconTM 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/

SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

***Actual Exam Questions**: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps**: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests**: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success**: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:** Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support**: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*