



EC-Council

Exam Questions 312-39

Certified SOC Analyst (CSA)

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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

Answer: D

NEW QUESTION 2

The Syslog message severity levels are labelled from level 0 to level 7. What does level 0 indicate?

- A. Alert
- B. Notification
- C. Emergency
- D. Debugging

Answer: B

NEW QUESTION 3

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 4

Which of the following contains the performance measures, and proper project and time management details?

- A. Incident Response Policy
- B. Incident Response Tactics
- C. Incident Response Process
- D. Incident Response Procedures

Answer: D

NEW QUESTION 5

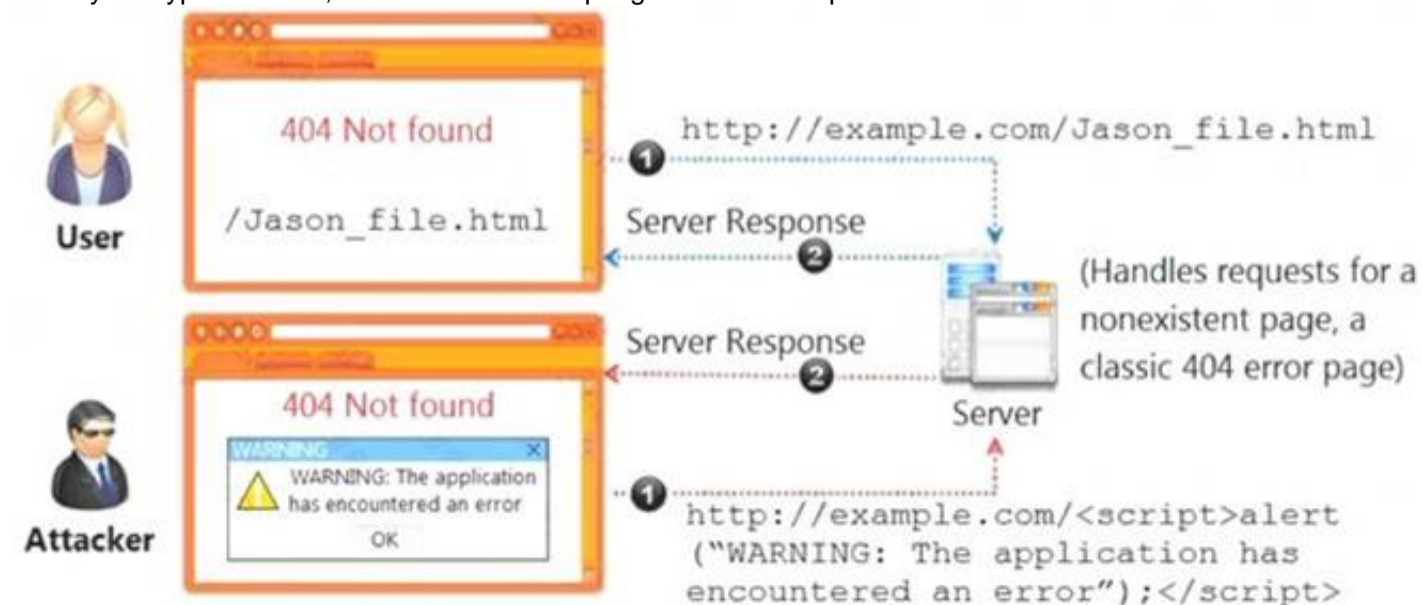
Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?

- 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

NEW QUESTION 6

Identify the type of attack, an attacker is attempting on www.example.com website.



- A. Cross-site Scripting Attack
- B. Session Attack

- C. Denial-of-Service Attack
- D. SQL Injection Attack

Answer: A

NEW QUESTION 7

What does [-n] in the following checkpoint firewall log syntax represents?

fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification_scheme_file] [-m unification_mode(initial|semi|raw)] [-a] [-k (alert name|all)] [-g] [logfile]

- A. Speed up the process by not performing IP addresses DNS resolution in the Log files
- B. Display both the date and the time for each log record
- C. Display account log records only
- D. Display detailed log chains (all the log segments a log record consists of)

Answer: A

NEW QUESTION 8

Which of the following technique involves scanning the headers of IP packets leaving a network to make sure that the unauthorized or malicious traffic never leaves the internal network?

- A. Egress Filtering
- B. Throttling
- C. Rate Limiting
- D. Ingress Filtering

Answer: A

NEW QUESTION 9

Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?

- A. Rule-based detection
- B. Heuristic-based detection
- C. Anomaly-based detection
- D. Signature-based detection

Answer: C

NEW QUESTION 10

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: B

NEW QUESTION 10

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

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

Answer: A

NEW QUESTION 11

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. File Injection Attacks
- D. LDAP Injection Attacks

Answer: B

NEW QUESTION 14

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

- A. Identifying the monitoring Requirements

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

Answer: D

NEW QUESTION 17

Which of the following technique protects from flooding attacks originated from the valid prefixes (IP addresses) so that they can be traced to its true source?

- A. Rate Limiting
- B. Egress Filtering
- C. Ingress Filtering
- D. Throttling

Answer: C

NEW QUESTION 18

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 22

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

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

Answer: C

NEW QUESTION 26

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 30

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 31

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

NEW QUESTION 36

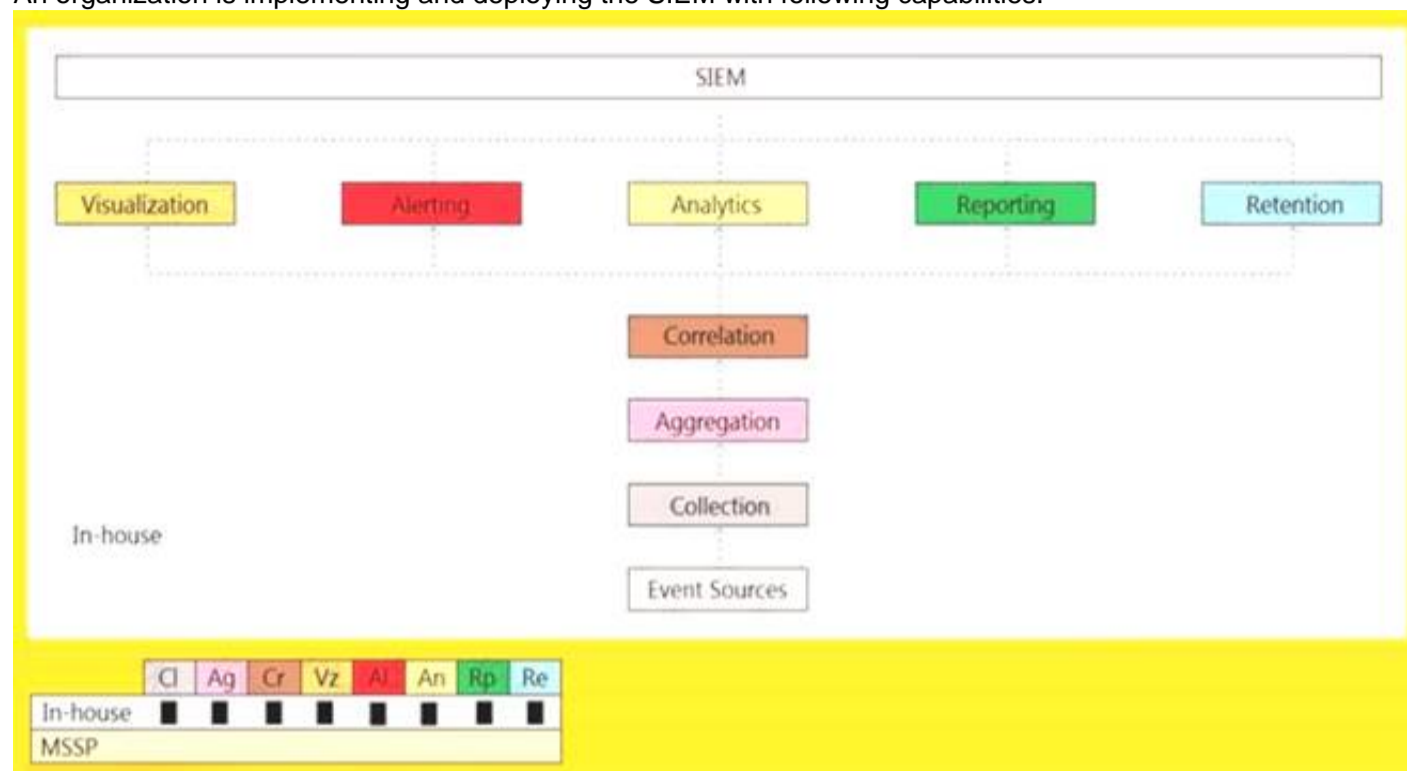
Which encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal?

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

Answer: D

NEW QUESTION 39

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



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

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

Answer: A

NEW QUESTION 43

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. IV
- C. II
- D. I

Answer: D

NEW QUESTION 48

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 53

Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex `/((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[\^n]+((\%3E)|>)/.`

What does this event log indicate?

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

Answer: C

NEW QUESTION 55

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

NEW QUESTION 59

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 62

John, a SOC analyst, while monitoring and analyzing Apache web server logs, identified an event log matching Regex `/(\.|\(|\)|\%25)2E)(\(|\)|\%25)2E)(\(|\)|\%25)2F|\\(|\)|\%25)5C)/i`.
What does this event log indicate?

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

Answer: A

NEW QUESTION 67

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. COBIT
- B. ITIL
- C. SSE-CMM
- D. SOC-CMM

Answer: C

NEW QUESTION 71

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

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

Answer: C

NEW QUESTION 72

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: B

NEW QUESTION 74

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: C

NEW QUESTION 79

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 84

Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for further investigation and confirmation. Charline, after a thorough investigation, confirmed the incident and assigned it with an initial priority. What would be her next action according to the SOC workflow?

- A. She should immediately escalate this issue to the management
- B. She should immediately contact the network administrator to solve the problem
- C. She should communicate this incident to the media immediately
- D. She should formally raise a ticket and forward it to the IRT

Answer: B

NEW QUESTION 89

InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC. Identify the job role of John.

- A. Security Analyst – L1
- B. Chief Information Security Officer (CISO)
- C. Security Engineer
- D. Security Analyst – L2

Answer: B

NEW QUESTION 91

Which of the following attacks causes sudden changes in file extensions or increase in file renames at rapid speed?

- A. Ransomware Attack
- B. DoS Attack
- C. DHCP starvation Attack
- D. File Injection Attack

Answer: A

NEW QUESTION 93

In which phase of Lockheed Martin's – Cyber Kill Chain Methodology, adversary creates a deliverable malicious payload using an exploit and a backdoor?

- A. Reconnaissance
- B. Delivery
- C. Weaponization
- D. Exploitation

Answer: B

NEW QUESTION 98

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 100

Which of the following is a Threat Intelligence Platform?

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

Answer: A

NEW QUESTION 101

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

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

Answer: C

NEW QUESTION 103

Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?

- A. Containment → Incident Recording → Incident Triage → Preparation → Recovery → Eradication → Post-Incident Activities
- B. Preparation → Incident Recording → Incident Triage → Containment → Eradication → Recovery → Post-Incident Activities
- C. Incident Triage → Eradication → Containment → Incident Recording → Preparation → Recovery → Post-Incident Activities
- D. Incident Recording → Preparation → Containment → Incident Triage → Recovery → Eradication → Post-Incident Activities

Answer: B

NEW QUESTION 107

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. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.
- B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.
- C. DNS/ Web Server logs with IP addresses.
- D. Apache/ Web Server logs with IP addresses and Host Name.

Answer: D

NEW QUESTION 109

Emmanuel is working as a SOC analyst in a company named Tobey Tech. The manager of Tobey Tech recently recruited an Incident Response Team (IRT) for his company. In the process of collaboration with the IRT, Emmanuel just escalated an incident to the IRT.

What is the first step that the IRT will do to the incident escalated by Emmanuel?

- A. Incident Analysis and Validation
- B. Incident Recording
- C. Incident Classification
- D. Incident Prioritization

Answer: C

NEW QUESTION 113

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 115

John, SOC analyst wants to monitor the attempt of process creation activities from any of their Windows endpoints.

Which of following Splunk query will help him to fetch related logs associated with process creation?

- A. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*\$)
- B. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*\$)
- C. index=windows LogName=Security EventCode=3688 NOT (Account_Name=*\$)
- D. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*\$)

Answer: B

NEW QUESTION 119

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 120

.....

Relate Links

100% Pass Your 312-39 Exam with Exam Bible Prep Materials

<https://www.exambible.com/312-39-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>