



## EC-Council

### Exam Questions 312-39

Certified SOC Analyst (CSA)

#### NEW QUESTION 1

What is the correct sequence of SOC Workflow?

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

**Answer:** A

#### NEW QUESTION 2

Which of the following Windows Event Id will help you monitors file sharing across the network?

- A. 7045
- B. 4625
- C. 5140
- D. 4624

**Answer:** C

#### NEW QUESTION 3

Jason, a SOC Analyst with Maximus Tech, was investigating Cisco ASA Firewall logs and came across the following log entry:

May 06 2018 21:27:27 asa 1: %ASA -5 – 11008: User 'enable\_15' executed the 'configure term' command What does the security level in the above log indicates?

- A. Warning condition message
- B. Critical condition message
- C. Normal but significant message
- D. Informational message

**Answer:** A

#### NEW QUESTION 4

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 5

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 6

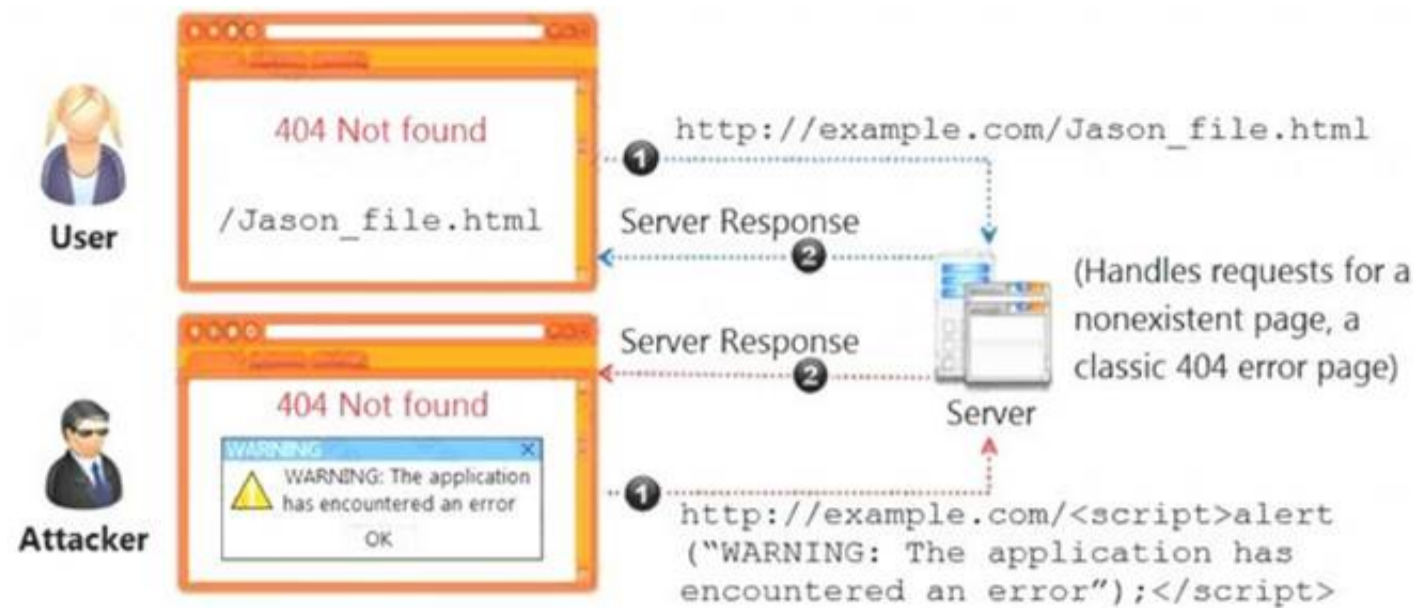
Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?

- 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 7

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 8

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:** A

#### NEW QUESTION 9

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 10

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

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 13

Which of the following directory will contain logs related to printer access?

- A. /var/log/cups/Printer\_log file
- B. /var/log/cups/access\_log file
- C. /var/log/cups/accesslog file
- D. /var/log/cups/Printeraccess\_log file

**Answer:** A

#### NEW QUESTION 15

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 19

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 23

David is a SOC analyst in Karen Tech. One day an attack is initiated by the intruders but David was not able to find any suspicious events. This type of incident is categorized into?

- A. True Positive Incidents
- B. False positive Incidents
- C. True Negative Incidents
- D. False Negative Incidents

**Answer:** C

#### NEW QUESTION 26

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 31

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

#### NEW QUESTION 35

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 36

Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:

`http://www.terabytes.com/process.php/../../../../etc/passwd`

- A. Directory Traversal Attack
- B. SQL Injection Attack
- C. Denial-of-Service Attack
- D. Form Tampering Attack

**Answer:** B

#### NEW QUESTION 40

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 42

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 45

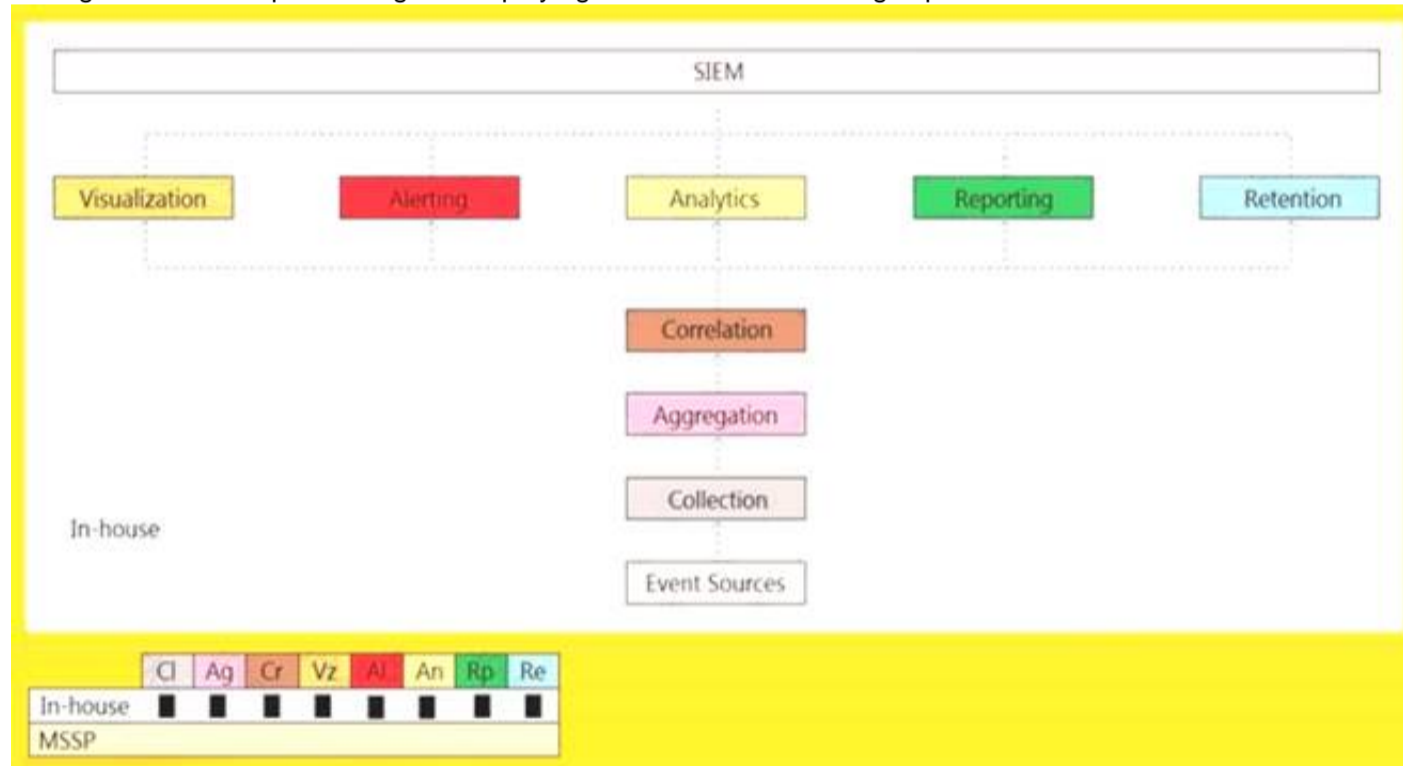
Identify the HTTP status codes that represents the server error.

- A. 2XX
- B. 4XX
- C. 1XX
- D. 5XX

**Answer:** D

#### NEW QUESTION 47

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 51

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 52

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 58

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

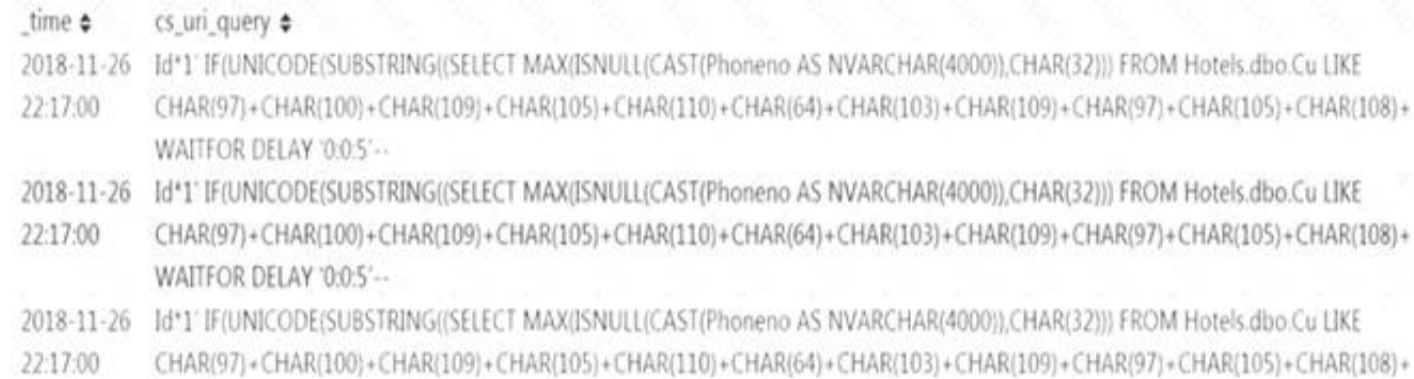
What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?

- 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 62

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



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 65

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:** B

#### NEW QUESTION 66

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

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 74

Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads. What does this indicate?

- A. Concurrent VPN Connections Attempt
- B. DNS Exfiltration Attempt
- C. Covering Tracks Attempt
- D. DHCP Starvation Attempt

**Answer:** B

#### NEW QUESTION 75

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 79

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 83

Wesley is an incident handler in a company named Maddison Tech. One day, he was learning techniques for eradicating the insecure deserialization attacks. What among the following should Wesley avoid from considering?

- A. Deserialization of trusted data must cross a trust boundary
- B. Understand the security permissions given to serialization and deserialization
- C. Allow serialization for security-sensitive classes
- D. Validate untrusted input, which is to be serialized to ensure that serialized data contain only trusted classes

**Answer:** C

#### NEW QUESTION 84

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

**Answer:** C

#### NEW QUESTION 85

Which of the following attack can be eradicated by disabling of "allow\_url\_fopen and allow\_url\_include" in the php.ini file?

- A. File Injection Attacks
- B. URL Injection Attacks
- C. LDAP Injection Attacks
- D. Command Injection Attacks

**Answer:** B

#### NEW QUESTION 90

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 94**

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 95**

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 96**

.....

## 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](#)**