Download Eccouncil 312-39 Exam Dumps Free

Shared by Walter on 17-06-2026

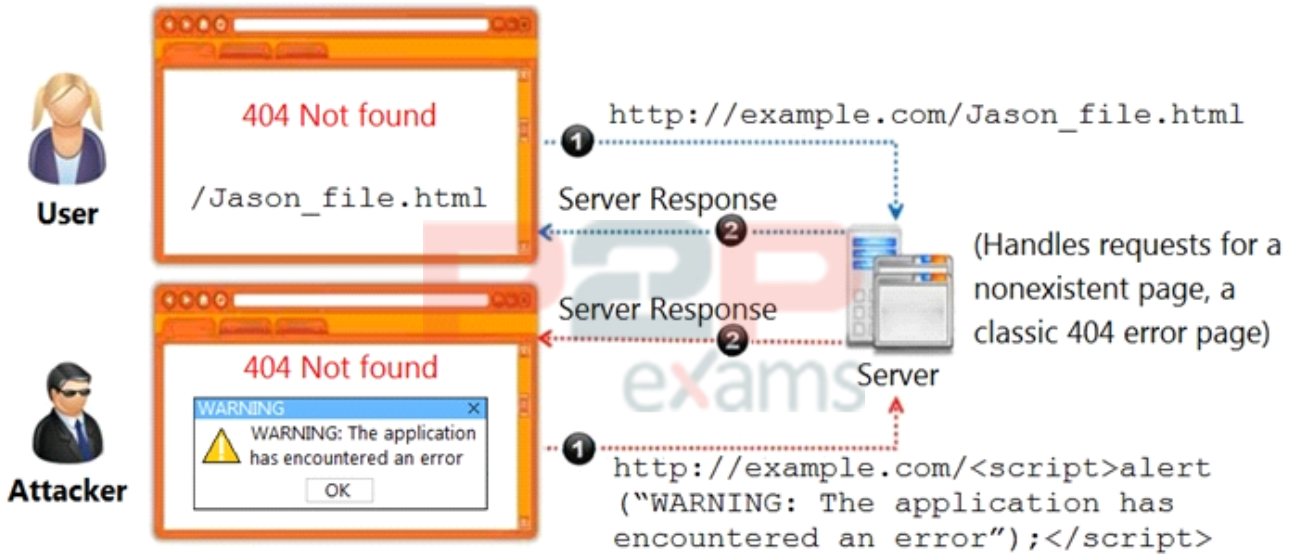
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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



Options:

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

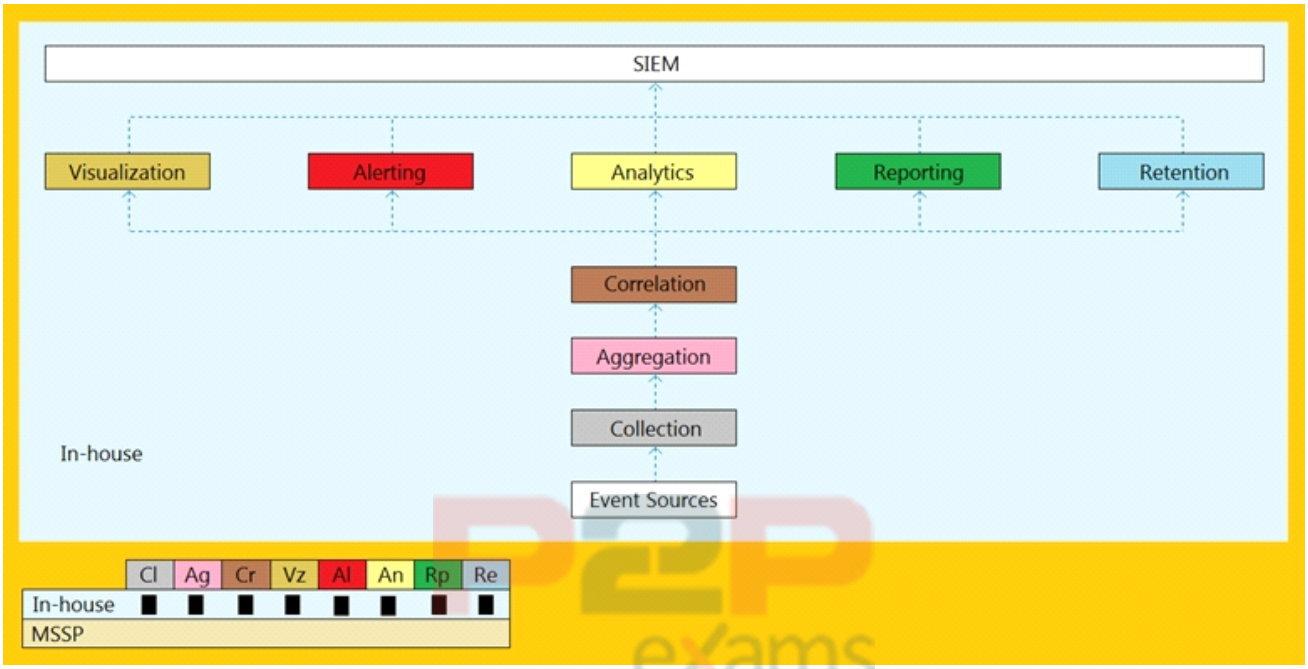
Answer:

A

Question 2

Question Type: MultipleChoice

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



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

Options:

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

Answer:

C

Question 3

Question Type: MultipleChoice

Identify the HTTP status codes that represents the server error.

Options:

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

Answer:

D

Question 4

Question Type: MultipleChoice

Which of the following threat intelligence is used by a SIEM for supplying the analysts with context and "situational awareness" by using threat actor TTPs, malware campaigns, tools used by threat actors.

1. Strategic threat intelligence

2. Tactical threat intelligence

3. Operational threat intelligence

4. Technical threat intelligence

Options:

A- 2 and 3
B- 1 and 3
C- 3 and 4
D- 1 and 2

Answer:

A

Question 5

Question Type: MultipleChoice

Which of the following framework describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering?

Options:

A- COBIT
B- ITIL

C- SSE-CMM
D- SOC-CMM

Answer:

C

Question 6

Question Type: MultipleChoice

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

Options:

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

Answer:

A

Question 7

Question Type: MultipleChoice

Which option best directory will contain logs related to printer access?

Options:

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:

B

Question 8

Question Type: MultipleChoice

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.

Options:

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

Answer:

B

Question 9

Question Type: MultipleChoice

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?

Options:

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

Answer:

D

Question 10

Question Type: MultipleChoice

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?

Options:

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

Answer:

C

Question 11

Question Type: MultipleChoice

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

Options:

A- CrowdStrike FalconTM Orchestrator
B- Symantec Secure Web Gateway
C- Smoothwall SWG
D- Proxy Workbench

Answer:

A

Question 12

Question Type: MultipleChoice

What does Windows event ID 4740 indicate?

Options:

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