312-39Q&As

Certified SOC Analyst (CSA)

Pass Pegasystems 312-39 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/312-39.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Pegasystems Official Exam Center

QUESTION 1

Harley is working as a SOC analyst with Powell Tech. Powell Inc. is using Internet Information Service (IIS) version 7.0 to host their website.

Where will Harley find the web server logs, if he wants to investigate them for any anomalies?

A. SystemDrive%\inetpub\logs\LogFiles\W3SVCN

B. SystemDrive%\LogFiles\inetpub\logs\W3SVCN

C. %SystemDrive%\LogFiles\logs\W3SVCN

D. SystemDrive%\ inetpub\LogFiles\logs\W3SVCN

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/sitedefaults/ logfile/

QUESTION 2

Which of the following attack can be eradicated by filtering improper XML syntax?

A. CAPTCHA Attacks

B. SQL Injection Attacks

C. Insufficient Logging and Monitoring Attacks

D. Web Services Attacks

Correct Answer: B

QUESTION 3

Which of the following formula represents the risk levels?

A. Level of risk = Consequence x Severity

B. Level of risk = Consequence x Impact

C. Level of risk = Consequence x Likelihood

D. Level of risk = Consequence x Asset Value

Correct Answer: B

QUESTION 4

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

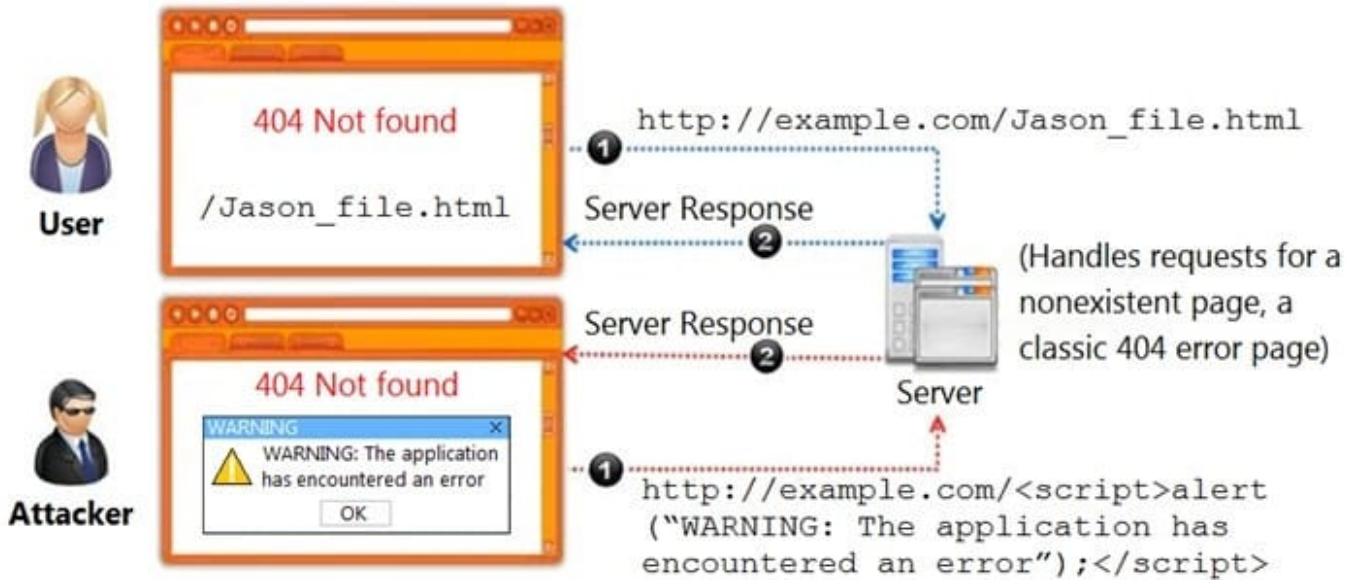
D. Intrusion Detection System

Correct Answer: C

Reference: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

QUESTION 5

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

Correct Answer: A

QUESTION 6

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

Correct Answer: C

Reference: http://www.mecs-press.org/ijcnis/ijcnis-v5-n5/IJCNIS-V5-N5-6.pdf (3)

QUESTION 7

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

Correct Answer: D

Reference: https://ktflash.gitbooks.io/ceh_v9/content/125_countermeasures.html

QUESTION 8

What is the process of monitoring and capturing all data packets passing through a given network using different tools?

A. Network Scanning

B. DNS Footprinting

C. Network Sniffing

D. Port Scanning

Correct Answer: C

Reference: https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types

QUESTION 9

Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.

A. Dictionary Attack

B. Rainbow Table Attack

C. Bruteforce Attack

D. Syllable Attack

Correct Answer: A

Reference: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic7-final/report.pdf

QUESTION 10

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

Correct Answer: A

Reference: https://www.eccouncil.org/wp-content/uploads/2019/02/ECIH-V2-Brochure.pdf

QUESTION 11

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

Correct Answer: A

QUESTION 12

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

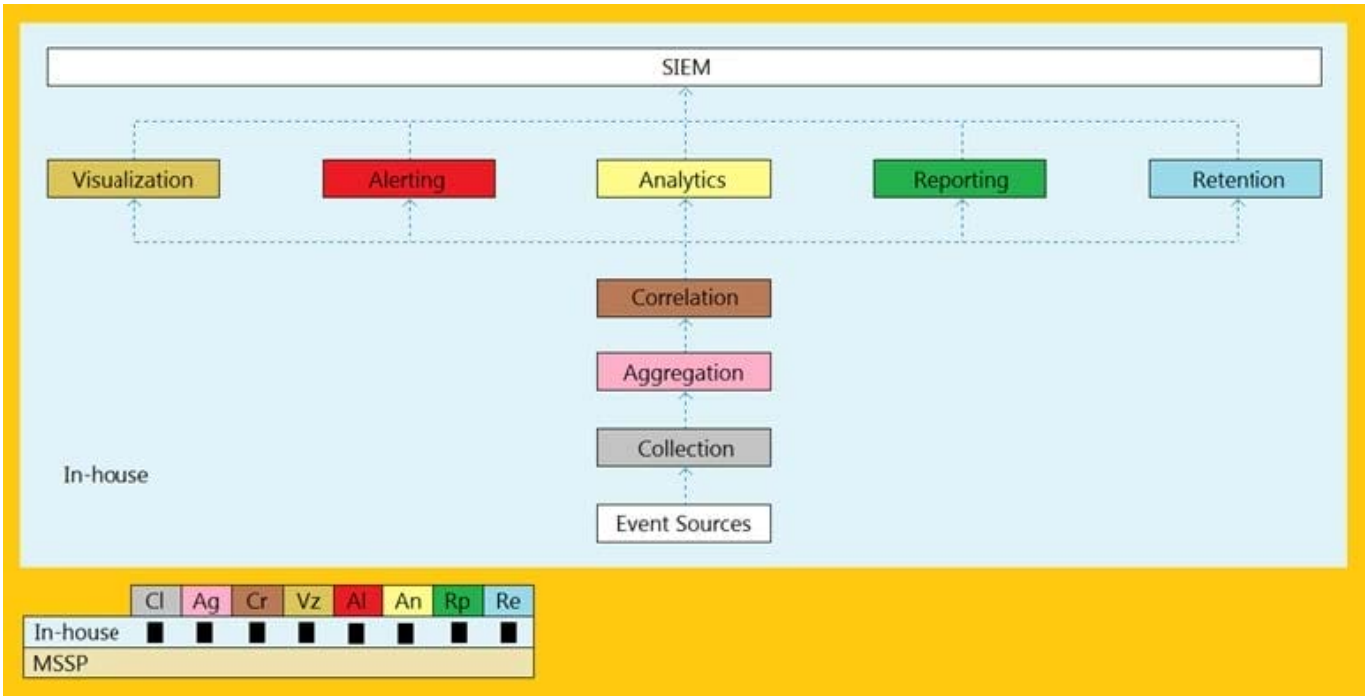
D. Session Management Attacks

Correct Answer: C

Reference: https://ktflash.gitbooks.io/ceh_v9/content/125_countermeasures.html

QUESTION 13

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

Correct Answer: A

QUESTION 14

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

A. 7045

B. 4625

C. 5140

D. 4624

Correct Answer: C

Reference: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5140

QUESTION 15

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

Correct Answer: C

Reference: https://www.recordedfuture.com/threat-intelligence/