312-39$^{Q\&As}$

Certified SOC Analyst (CSA)

Pass Pegasystems 312-39 Exam with 100% Guarantee

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

QUESTION 1

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

Correct Answer: A

QUESTION 2

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

Correct Answer: D

Reference: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101july2017.pdf

QUESTION 3

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

Correct Answer: A

QUESTION 4

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/

QUESTION 5

Which of the following are the responsibilities of SIEM Agents?

1.

Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.

2.

Normalizing data received from various devices sending data to SIEM before forwarding it to the central engine.

3.

Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.

4.

Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.

A. 1 and 2

B. 2 and 3

C. 1 and 4

D. 3 and 1

Correct Answer: C

QUESTION 6

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

Correct Answer: C

Reference: https://www.iso.org/standard/44716.html

QUESTION 7

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

Correct Answer: B

QUESTION 8

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

Correct Answer: B

Reference: https://www.exabeam.com/security-operations-center/security-operations-center-roles-andresponsibilities/

QUESTION 9

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 10

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

Correct Answer: A

QUESTION 11

Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses?

A. DHCP Starvation Attacks

B. DHCP Spoofing Attack

C. DHCP Port Stealing

D. DHCP Cache Poisoning

Correct Answer: A

Reference: https://www.cbtnuggets.com/blog/technology/networking/what-is-a-dhcp-starvation-attack

QUESTION 12

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

Correct Answer: C

QUESTION 13

Identify the HTTP status codes that represents the server error.

A. 2XX

B. 4XX

C. 1XX

D. 5XX

Correct Answer: D

Reference: https://www.tutorialspoint.com/http/http_status_codes.htm

QUESTION 14

Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As a part of threat intelligent strategy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in.

Which one of the following components he should include in the above threat intelligent strategy plan to make it effective?

A. Threat pivoting

B. Threat trending

C. Threat buy-in

D. Threat boosting

Correct Answer: C

QUESTION 15

Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

A. Failure Audit

B. Warning

C. Error

D. Information

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/windows/win32/eventlog/event-types