312-39 Q&As

Certified SOC Analyst (CSA)

Pass Pegasystems 312-39 Exam with 100% Guarantee

QUESTION 1

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 2

Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex /\\w*((\%27)|(\\\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix.

What does this event log indicate?

A. SQL Injection Attack

B. Parameter Tampering Attack

C. XSS Attack

D. Directory Traversal Attack

Correct Answer: A

Reference: https://community.broadcom.com/symantecenterprise/communities/community-home/ librarydocuments/viewdocument?DocumentKey=001f5e09-88b4-4a9a-b3104c20578eecf9andCommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68andtab=librarydocuments

QUESTION 3

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 4

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.

Correct Answer: D

QUESTION 5

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/