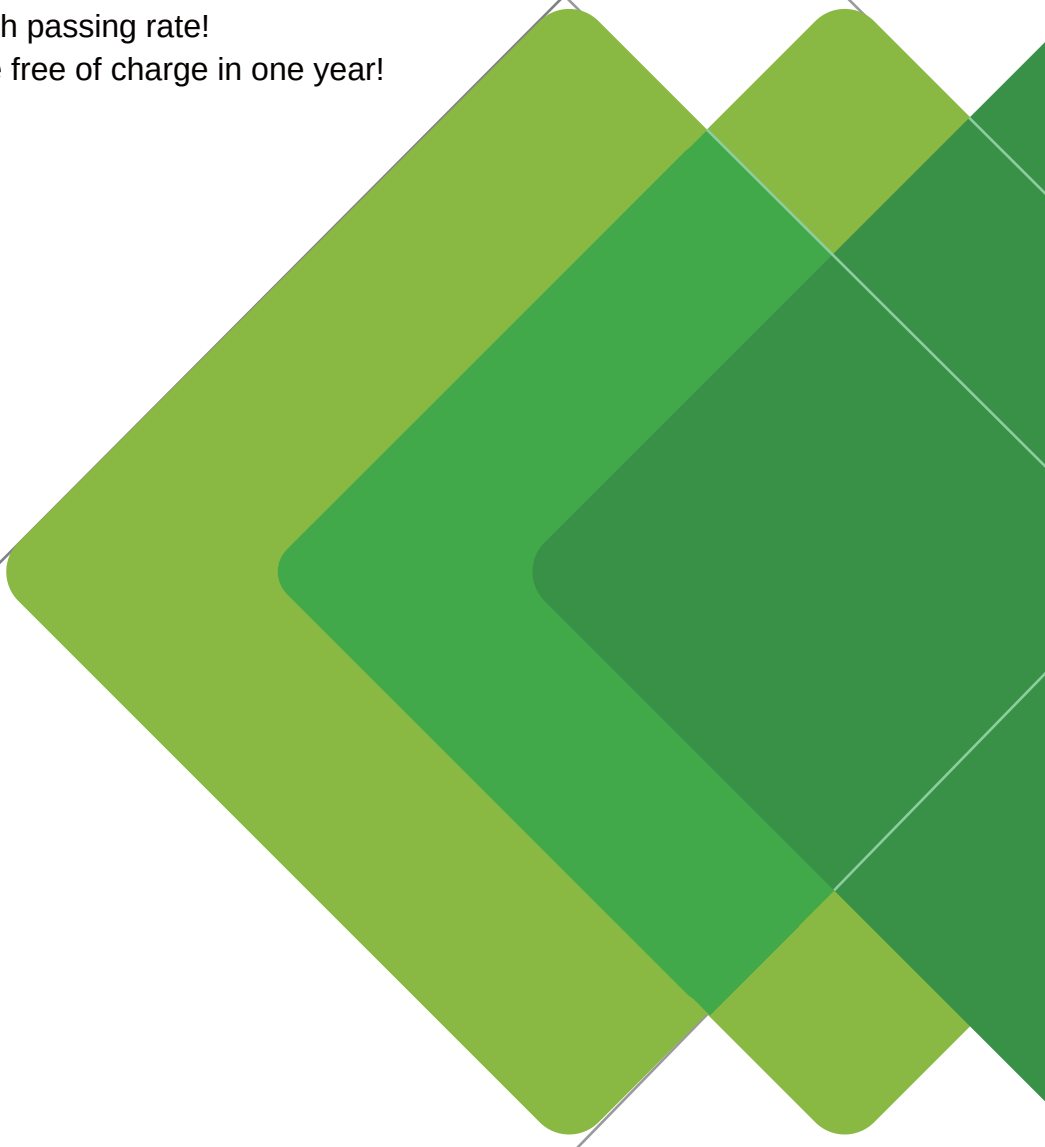
IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!



Exam : **312-39**

Title : Certified SOC Analyst (CSA)

Version : DEMO

1.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
Explanation:
Reference:
https://books.google.com.pk/books?id=PDR4nOAP8qUC&pg=PA87&lpg=PA87&dq=regex+/((%5C%253C)%7C<)((%5C%2569)%7Ci%7C(%5C%2549))((%5C%256D)%7Cm%7C(%5C%25 4D))((%5C%2567)%7Cg%7C(%5C%2547))%5B%5E%5Cn%5D%2B((%5C%253E)%7C>)/%7C&source=bl&ots=kOBHNfJmtq&sig=ACfU3U2CG_hELc1HMb1chdc9OS4ooXPlMg&hl=en&sa=X&ved=2ahUKEwjYwJmlt_buAhUFShUIHTBNAs8Q6AEwBXoECAUQAw#v=onepage&q&f=false

2.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
Answer: A

3.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
Answer: A
Explanation:
Reference: https://www.eccouncil.org/wp-content/uploads/2019/02/ECIH-V2-Brochure.pdf

4.Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?
A. Windows Event Log
B. Web Server Logs
C. Router Logs
D. Switch Logs
Answer: B

5.Emmanuel is working as a SOC analyst in a company named Tobey Tech. The manager of Tobey Tech

recently recruited an Incident Response Team (IRT) for his company. In the process of collaboration with the IRT, Emmanuel just escalated an incident to the IRT.
What is the first step that the IRT will do to the incident escalated by Emmanuel?
A. Incident Analysis and Validation
B. Incident Recording
C. Incident Classification
D. Incident Prioritization
Answer: A