Free Questions for 312-39 by go4braindumps

Shared by Moody on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

A- Broken Access Control Attacks

B- Web Services Attacks

C- XSS Attacks

D- Session Management Attacks

Answer:

C

Question 2

Question Type: MultipleChoice

Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

Options:

A- Hybrid Attack

B- Bruteforce Attack

C- Rainbow Table Attack

D- Birthday Attack

Answer:

B

Question 3

Question Type: **MultipleChoice**

Jony , a security analyst, while monitoring IIS logs, identified events shown in the figure below.

_time	cs_uri_query
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+ WAITFOR DELAY '0:0:5'--
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+ WAITFOR DELAY '0:0:5'--
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+

What does this event log indicate?

Options:

A- Parameter Tampering Attack

B- XSS Attack

C- Directory Traversal Attack

D- SQL Injection Attack

Answer:

A

Question 4

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 5

Question Type: MultipleChoice

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?

Options:

A- Incident Analysis and Validation

B- Incident Recording

C- Incident Classification

D- Incident Prioritization

Answer:

C

Question 6

Question Type: **MultipleChoice**

David is a SOC analyst in Karen Tech. One day an attack is initiated by the intruders but David was not able to find any suspicious events.

This type of incident is categorized into ?

Options:

A- True Positive Incidents

B- False positive Incidents

C- True Negative Incidents

D- False Negative Incidents

Answer:

C

Question 7

Question Type: **MultipleChoice**

Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for further investigation and confirmation. Charline, after a thorough investigation, confirmed the incident and assigned it with an initial priority.

What would be her next action according to the SOC workflow?

Options:

A- She should immediately escalate this issue to the management

B- She should immediately contact the network administrator to solve the problem

C- She should communicate this incident to the media immediately

D- She should formally raise a ticket and forward it to the IRT

Answer:

B

Question 8

Question Type: **MultipleChoice**

Which of the following tool can be used to filter web requests associated with the SQL Injection attack?

Options:

A- Nmap

B- UrlScan

C- ZAP proxy

D- Hydra

Answer:

B

Question 9

Question Type: **MultipleChoice**

Which of the following process refers to the discarding of the packets at the routing level without informing the source that the data did not reach its intended recipient?

Options:

A- Load Balancing

B- Rate Limiting

C- Black Hole Filtering

D- Drop Requests

Answer:

C

Question 10

Question Type: MultipleChoice

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?

Options:

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.

Answer:

D

Question 11

Question Type: **MultipleChoice**

Which of the following contains the performance measures, and proper project and time management details?

Options:

A- Incident Response Policy

B- Incident Response Tactics

C- Incident Response Process

D- Incident Response Procedures

Answer:

D

Question 12

Question Type: MultipleChoice

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?

Options:

A- Rate Limiting

B- Egress Filtering

C- Ingress Filtering

D- Throttling

Answer:

C