Free Questions for 312-39 by ebraindumps

Shared by Hicks on 05-09-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which alert should be given least priority as per effective alert triaging?

If the SIEM generates the following four alerts at the same time:

Options:

A) I.Firewall blocking traffic from getting into the network alerts

B) II.SQL injection attempt alerts

C) III.Data deletion attempt alerts

D) IV.Brute-force attempt alerts

Answer:

A

Question 2

Question Type: **MultipleChoice**

An attacker exploits the logic validation mechanisms of an e-commerce website. He successfully purchases a product worth $100 for $10 by modifying the URL exchanged between the client and the server.

Identify the attack depicted in the above scenario.

Options:

A) Denial-of-Service Attack

B) SQL Injection Attack

C) Parameter Tampering Attack

D) Session Fixation Attack

Section: (none)

Explanation

Answer:

D

Question 3

Question Type: MultipleChoice

An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted code at the end of the company's URL as follows:

Options:

A) Cross-site Scripting Attack

B) SQL Injection Attack

C) Denial-of-Service Attack

D) Session Attack

Answer:

D

Question 4

Question Type: **MultipleChoice**

Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:

Options:

A) Directory Traversal Attack

B) SQL Injection Attack

C) Denial-of-Service Attack

D) Form Tampering Attack

Answer:

B

Question 5

Question Type: **MultipleChoice**

An attacker exploits the logic validation mechanisms of an e-commerce website. He successfully purchases a product worth $100 for $10 by modifying the URL exchanged between the client and the server.

Identify the attack depicted in the above scenario.

Options:

A) Denial-of-Service Attack

B) SQL Injection Attack

C) Parameter Tampering Attack

D) Session Fixation Attack

Section: (none)

Explanation

Answer:

D

Question 6

Question Type: MultipleChoice

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?

Options:

A) SQL Injection Attack

B) Parameter Tampering Attack

C) XSS Attack

D) Directory Traversal Attack

Answer:

A

Question 7

Question Type: **MultipleChoice**

An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted code at the end of the company's URL as follows:

Options:

A) Cross-site Scripting Attack

B) SQL Injection Attack

C) Denial-of-Service Attack

D) Session Attack

Answer:

D

Question 8

Question Type: MultipleChoice

Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:

Options:

A) Directory Traversal Attack

B) SQL Injection Attack

C) Denial-of-Service Attack

D) Form Tampering Attack

Answer:

B

Question 9

Question Type: MultipleChoice

Which alert should be given least priority as per effective alert triaging?

If the SIEM generates the following four alerts at the same time:

Options:

A) I.Firewall blocking traffic from getting into the network alerts

B) II.SQL injection attempt alerts

C) III.Data deletion attempt alerts

D) IV.Brute-force attempt alerts

Answer:

A