Free Questions for CS0-002 by vceexamstest

Shared by Hughes on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

Options:

A- strings

B- head

C- fsstat

D- dd

Answer:

A

Question 2

Question Type: MultipleChoice

An organization is focused on restructuring its data governance programs and an analyst has been Tasked with surveying sensitive data within the organization. Which of the following is the MOST accurate method for the security analyst to complete this assignment?

Options:

A- Perform an enterprise-wide discovery scan.

B- Consult with an internal data custodian.

C- Review enterprise-wide asset Inventory.

D- Create a survey and distribute it to data owners.

Answer:

D

Question 3

Question Type: MultipleChoice

A SIEM analyst receives an alert containing the following URL:

http://companywebsite.com/displayPicture?filename=../../../etc/passwd

Which of the following BEST describes the attack?

Options:

A- Password spraying

B- Buffer overflow

C- insecure object access

D- Directory traversal

Answer:

D

Question 4

Question Type: **MultipleChoice**

A small organization has proprietary software that is used internally. The system has not been wen maintained and cannot be updated with the rest or the environment. Which of the following is the BEST solution?

Options:

A- virtualize the system and decommission the physical machine.

B- Remove it from the network and require air gapping.

C- Implement privileged access management for identity access.

D- Implement MFA on the specific system.

Answer:

B

Question 5

Question Type: MultipleChoice

A Chief Executive Officer (CEO) is concerned about the company's intellectual property being leaked to competitors. The security team performed an extensive review but did not find any indication of an outside breach. The data sets are currently encrypted using the Triple Data Encryption Algorithm. Which of the following courses of action is appropriate?

Options:

A- Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.

B- Enable data masking and reencrypt the data sets using AES-256.

C- Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.

D- Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.

Answer:

C

Question 6

Question Type: MultipleChoice

A security analyst has discovered malware is spreading across multiple critical systems and is originating from a single workstations, which belongs to a member of the cyber-infrastructure team who has legitimate administrator credentials. An analysis of the traffic indicates the workstation swept the networking looking for vulnerable hosts to infect. Which of the following would have worked BEST to prevent the spread of this infection?

Options:

A- Vulnerability scans of the network and proper patching.

B- A properly configured and updated EDR solution.

C- A honeypot used to catalog the anomalous behavior and update the IPS.

D- Logical network segmentation and the use of jump boxes

Answer:

A

Question 7

Question Type: **MultipleChoice**

An analyst has received a notification about potential malicious activity against a web server. The analyst logs in to a central log collection server and runs the following command: "cat access.log.1 | grep "union". The output shown below appears:

-- -- [31/Jan/2020:10:02:31 --0400] "Get /cgi-bin/backend1.sh?id=%20union%20select%20192.168.60.50 HTTP/1.1"

Which of the following attacks has occurred on the server?

Options:

A- Cross-site request forgery

B- SQL injection

C- Cross-site scripting

D- Directory traversal

Answer:

C

Question 8

Question Type: **MultipleChoice**

The management team assigned the following values to an inadvertent breach of privacy regulations during the original risk assessment:

Probability = 25%

Magnitude = $1,015 per record

Total records = 10,000

Two breaches occurred during the fiscal year. The first compromised 35 records, and the second compromised 65 records. Which of the following is the value of the records that were compromised?

Options:

A- $10,150

B- $25,375

C- $101,500

D- $2,537,500

Answer:

A

Question 9

Question Type: **MultipleChoice**

A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

Options:

A- Static analysis

B- Dynamic analysis

C- Regression testing

D- User acceptance testing

Answer:

C

Question 10

Question Type: **MultipleChoice**

A company's change management team has asked a security analyst to review a potential change to the email server before it is released into production. The analyst reviews the following change request:

Change request date:	2020-01-30
Change requester:	Cindy Richardson
Change asset:	WIN2K-EMAIL001
Change requested:	Modify the following SPF record to change +all to –all

Which of the following is the MOST likely reason for the change?

Options:

A- To reject email from servers that are not listed in the SPF record

B- To reject email from email addresses that are not digitally signed.

C- To accept email to the company's domain.

D- To reject email from users who are not authenticated to the network.

Answer:

A

Question 11

Question Type: MultipleChoice

An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization's network. Which of the following approaches should the security analyst recommend?

Options:

A- Use the MITRE ATT&CK framework to develop threat models.

B- Conduct internal threat research and establish indicators of compromise.

C- Review the perimeter firewall rules to ensure rule-set accuracy.

D- Use SCAP scans to monitor for configuration changes on the network.

Answer:

D