CAS-003$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An engineer wants to assess the OS security configurations on a company\\'s servers. The engineer has downloaded some files to orchestrate configuration checks When the engineer opens a file in a text editor, the following excerpt appears:

```
<?xml version="1.0" encoding="UTF-8"?>
<cdf:Benchmark id="server-check" resolved="0" xml:lang="en">
        ...
        xsi:schemaLocation="http://checklists.nist.gov/xccdf/1.1" xccdf-1.1.xsd
        ...
</cdf:Benchmark>
```

Which of the following capabilities would a configuration compliance checker need to support to interpret this file?

A. Nessus

B. Swagger file

C. SCAP

D. Netcat

E. WSDL

Correct Answer: C

QUESTION 2

An organization is evaluating options related to moving organizational assets to a cloud-based environment using an IaaS provider. One engineer has suggested connecting a second cloud environment within the organization\\'s existing facilities to capitalize on available datacenter space and resources. Other project team members are concerned about such a commitment of organizational assets, and ask the Chief Security Officer (CSO) for input. The CSO explains that the project team should work with the engineer to evaluate the risks associated with using the datacenter to implement:

A. a hybrid cloud.

B. an on-premises private cloud.

C. a hosted hybrid cloud.

D. a private cloud.

Correct Answer: A

QUESTION 3

The IT Security Analyst for a small organization is working on a customer\\'s system and identifies a possible intrusion in

a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.

B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.

C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.

D. Refer the issue to management for handling according to the incident response process.

Correct Answer: D

The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer\\'s system. Therefore, this IT Security Analyst does not know what the customer\\'s incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.

QUESTION 4

A newly hired Chief Information Security Officer (CISO) is reviewing the organization\\'s security budget from the previous year. The CISO notices $100,000 worth of fines were paid for not properly encrypting outbound email messages. The CISO expects next year\\'s costs associated with fines to double and the volume of messages to increase by 100%. The organization sent out approximately 25,000 messages per year over the last three years. Given the table below:

Security product	Hardware price	Installation fee	Cost per message	Throughput	MTBF
DLP Vendor A	$50,000	$25,000	$1	100Mbps	10000 hours
DLP Vendor B	$38,000	$10,000	$2	50Mbps	8000 hours
DLP Vendor C	$45,000	$30,000	$1	70Mbps	7000 hours
DLP Vendor D	$40,000	$60,000	$0.50	100Mbps	7000 hours

Which of the following would be BEST for the CISO to include in this year\\'s budget?

A. A budget line for DLP Vendor A

B. A budget line for DLP Vendor B

C. A budget line for DLP Vendor C

D. A budget line for DLP Vendor D

E. A budget line for paying future fines

Correct Answer: A

QUESTION 5

A cybersecurity analyst is conducting packet analysis on the following:

Time	Source	Destination	Info
0.000673	00:48:c2:5f:39:57	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:57
0.001173	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.6 is at 00:48:c2:5f:39:9a
0.002346	00:48:c2:5f:39:2b	00:43:b3:3f:23:e3	172.16.1.12 is at 00:48:c2:5f:39:2b
0.005123	00:48:c2:5f:39:42	00:43:b3:3f:23:e3	172.16.1.13 is at 00:48:c2:5f:39:42
0.010281	00:48:c2:5f:39:6b	00:43:b3:3f:23:e3	172.16.1.2 is at 00:48:c2:5f:39:6b
0.021597	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a
0.044812	00:48:c2:5f:39:3c	00:43:b3:3f:23:e3	172.16.1.21 is at 00:48:c2:5f:39:3c
0.06512	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a

Which of the following is occurring in the given packet capture?

A. ARP spoofing B. Broadcast storm

C. Smurf attack

D. Network enurneration

E. Zero-day exploit

Correct Answer: A