# CAS-004 Q&As

CompTIA Advanced Security Practitioner (CASP+)

## Pass CompTIA CAS-004 Exam with 100% Guarantee

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

**https://www.passapply.com/cas-004.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

An organization developed an incident response plan. Which of the following would be BEST to assess the effectiveness of the plan?

A. Requesting a third-party review

B. Generating a checklist by organizational unit

C. Establishing role succession and call lists

D. Creating a playbook

E. Performing a tabletop exercise

Correct Answer: E

**QUESTION 2**

Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.

Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement rate limiting on the API.

B. Implement geoblocking on the WAF.

C. Implement OAuth 2.0 on the API.

D. Implement input validation on the API.

Correct Answer: A

**QUESTION 3**

A security analyst is reviewing SIEM events and is uncertain how to handle a particular event. The file is reviewed with the security vendor who is aware that this type of file routinely triggers this alert. Based on this information, the security analyst acknowledges this alert. Which of the following event classifications is MOST likely the reason for this action?

A. True negative

B. False negative

C. False positive

D. Non-automated response

Correct Answer: C

**QUESTION 4**

After installing an unapproved application on a personal device, a Chief Executive Officer reported an incident to a security analyst. This device is not controlled by the MDM solution, as stated in the BVOD policy. However, the device contained critical confidential information. The cyber incident response team performed the analysis on the device and found the following log: Wed 12 Dec 2020 10:00:03 Unknown sources is now enabled on this device.

Which of the following is the MOST likely reason for the successful attack?

A. Lack of MDM controls

B. Auto-join hotspots enabled

C. Sideloading

D. Lack of application segmentation

Correct Answer: C

The enabling of "Unknown sources" suggests that an application was installed from outside the official app store, which can introduce significant security risks, especially if the source of the application isn\\'t trusted. This process is known as sideloading.

**QUESTION 5**

A company publishes several APIs for customers and is required to use keys to segregate customer data sets. Which of the following would be BEST to use to store customer keys?

A. A trusted platform module

B. A hardware security module

C. A localized key store

D. A public key infrastructure

Correct Answer: B

Reference: https://developer.android.com/studio/publish/app-signing