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.pass4itsure.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

A security manager is determining the best DLP solution for an enterprise A list of requirements was created to use during the source selection. The security manager wants to confirm a solution exists for the requirements that have been defined. Which of the following should the security manager use?

A. NDA

B. RFP

C. RFQ

D. MSA

E. RFI

Correct Answer: E

QUESTION 2

The following has been discovered in an internally developed application:

Error - Memory allocated but not freed:

```
char *myBuffer = malloc(BUFFER_SIZE);

if (myBuffer != NULL) {

*myBuffer = STRING_WELCOME_MESSAGE;

printf("Welcome to: %s\n", myBuffer);

}

exit(0);
```

Which of the following security assessment methods are likely to reveal this security weakness? (Select TWO).

A. Static code analysis

B. Memory dumping

C. Manual code review

D. Application sandboxing

E. Penetration testing

F. Black box testing

Correct Answer: AC

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization. Application code review ?whether manual or static will reveal the type of security weakness as shown in the exhibit.

QUESTION 3

An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user\\'s accounts is sensitive, and therefore, the organization wants to comply with the following requirements:

Active full-device encryption Enabled remote-device wipe Blocking unsigned applications Containerization of email, calendar, and contacts

Which of the following technical controls would BEST protect the data from attack or loss and meet the above requirements?

A. Require frequent password changes and disable NFC.

B. Enforce device encryption and activate MAM.

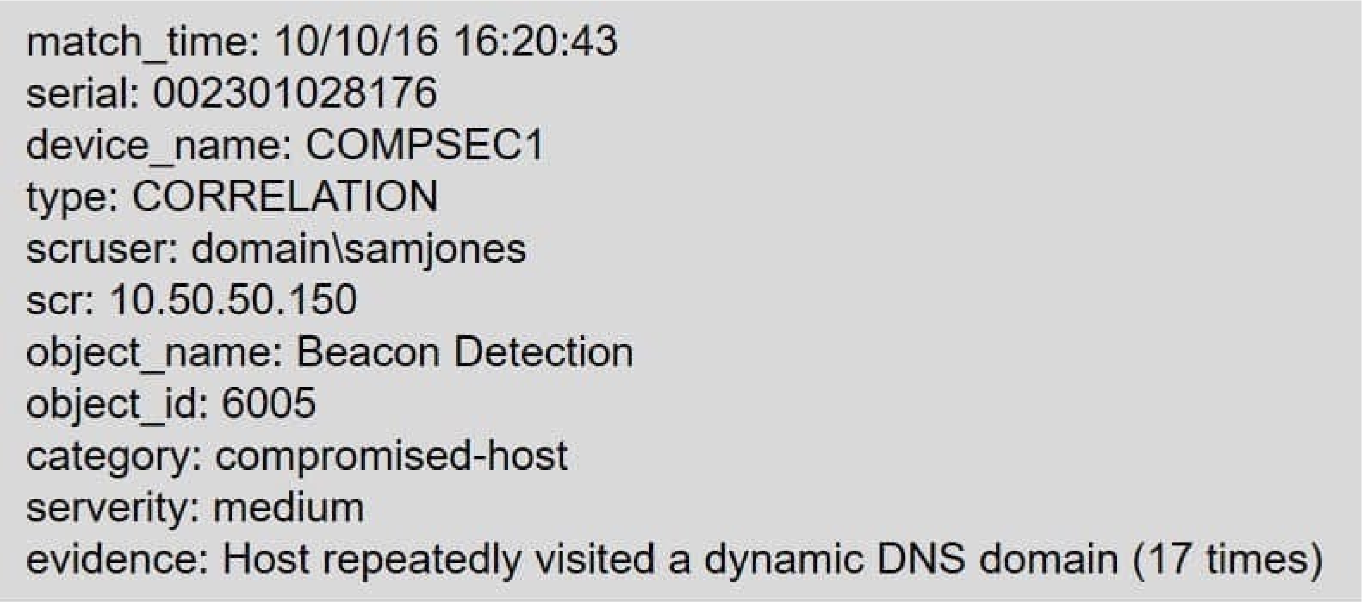
C. Install a mobile antivirus application.

D. Configure and monitor devices with an MDM.

Correct Answer: B

QUESTION 4

A technician receives the following security alert from the firewall\\'s automated system:



```
match_time: 10/10/16 16:20:43
serial: 002301028176
device_name: COMPSEC1
type: CORRELATION
scruser: domain\samjones
scr: 10.50.50.150
object_name: Beacon Detection
object_id: 6005
category: compromised-host
serverity: medium
evidence: Host repeatedly visited a dynamic DNS domain (17 times)
```

After reviewing the alert, which of the following is the BEST analysis?

A. This alert is false positive because DNS is a normal network function.

B. This alert indicates a user was attempting to bypass security measures using dynamic DNS.

C. This alert was generated by the SIEM because the user attempted too many invalid login attempts.

D. This alert indicates an endpoint may be infected and is potentially contacting a suspect host.

Correct Answer: B

QUESTION 5

An organization is concerned that its hosted web servers are not running the most updated version of software. Which of the following would work BEST to help identify potential vulnerabilities?

A. hping3 -S comptia.org -p 80

B. nc -1 -v comptia.org -p 80

C. nmap comptia.org -p 80 -sV

D. nslookup -port=80 comptia.org

Correct Answer: C