CAS-003Q&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.passapply.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A vendor develops a mobile application for global customers. The mobile application supports advanced encryption of data between the source (the mobile device) and the destination (the organization\\'s ERP system).

As part of the vendor\\'s compliance program, which of the following would be important to take into account?

A. Mobile tokenization

B. Export controls

C. Device containerization

D. Privacy policies

Correct Answer: D

QUESTION 2

Company A is establishing a contractual with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights. Which of the following documents will MOST likely contain these elements

A. Company A-B SLA v2.docx

B. Company A OLA v1b.docx

C. Company A MSA v3.docx

D. Company A MOU v1.docx

E. Company A-B NDA v03.docx

Correct Answer: A

QUESTION 3

A hospital is deploying new imaging softwares that requires a web server for access to image for both local and remote users. The web server allows user authentication via secure LDAP. The information security officer wants to ensure the server does not allow unencrypted access to the imaging server by using Nmap to gather additional information. Given the following:

1.

The imaging server IP is 192.168.101.24

2.

The domain controller IP is 192.168.100.1

3.

The client machine IP is 192.168.200.37

Which of the following should be used to confirm this is the only open post on the web server?

A. nmap "p 80,443 192.168.101.24

B. nmap "p 80,443,389,636 192.168.100.1

C. nmap "p 80,389 192.168.200.37

D. nmap "p" 192.168.101.24

Correct Answer: B

QUESTION 4

A company\\'s claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that approved to be claim form, but it installed malicious software on the employee\\'s laptop when was opened.

A. Impalement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.

B. Required all laptops to connect to the VPN before accessing email.

C. Implement cloud-based content filtering with sandboxing capabilities.

D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

Correct Answer: C

QUESTION 5

The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show the following:

90.76.165.40 -- [08/Mar/2014:10:54:04] "GET calendar.php?create%20table%20hidden HTTP/1.1" 200 5724

90.76.165.40 -- [08/Mar/2014:10:54:05] "GET ../../../root/.bash_history HTTP/1.1" 200 5724

90.76.165.40 -- [08/Mar/2014:10:54:04] "GET index.php?user;Creat; HTTP/1.1" 200 5724 The security administrator also inspects the following file system locations on the database server using the command `ls -al /root\\' drwxrwxrwx 11 root root 4096 Sep 28 22:45 . drwxr-xr-x 25 root root 4096 Mar 8 09:30 .. -rws------ 25 root root 4096 Mar 8 09:30 .bash_history -rw------- 25 root root 4096 Mar 8 09:30 .bash_history -rw------- 25 root root 4096 Mar 8 09:30 .profile -rw------- 25 root root 4096 Mar 8 09:30 .ssh Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).

A. Privilege escalation

B. Brute force attack

C. SQL injection

D. Cross-site scripting

E. Using input validation, ensure the following characters are sanitized:

F. Update crontab with: find / \(-perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh

G. Implement the following PHP directive: $clean_user_input = addslashes($user_input)

H. Set an account lockout policy

Correct Answer: AF

This is an example of privilege escalation.

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

The question states that the web server communicates with the database server via an account with SELECT only privileges. However, the privileges listed include read, write and execute (rwx). This suggests the privileges have been

`escalated\\'.

Now that we know the system has been attacked, we should investigate what was done to the system.

The command "Update crontab with: find / \(-perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh" is used to find all the files that are setuid enabled. Setuid means set user ID upon execution. If the setuid bit is turned on for a file, the user

executing that executable file gets the permissions of the individual or group that owns the file.

CAS-003 PDF Dumps CAS-003 Practice Test CAS-003 Braindumps