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

A security tester is testing a website and performs the following manual query:

https://www.comptia.com/cookies.jsp?products=5%20and%201=1

The following response is received in the payload:

"ORA-000001: SQL command not properly ended"

Which of the following is the response an example of?

A. Fingerprinting

B. Cross-site scripting

C. SQL injection

D. Privilege escalation

Correct Answer: A

This is an example of Fingerprinting. The response to the code entered includes "ORA-000001" which tells the attacker that the database software being used is Oracle.

Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished "passively" by sniffing network packets passing between hosts, or it can be accomplished "actively" by transmitting specially created packets to the target machine and analyzing the response.

QUESTION 2

An internal application has been developed to increase the efficiency of an operational process of a global manufacturer. New code was implemented to fix a security bug, but it has caused operations to halt. The executive team has decided fixing the security bug is less important than continuing operations.

Which of the following would BEST support immediate rollback of the failed fix? (Choose two.)

A. Version control

B. Agile development

C. Waterfall development

D. Change management

E. Continuous integration

Correct Answer: AD

QUESTION 3

A system administrator recently conducted a vulnerability scan of the internet. Subsequently, the organization was successfully attacked by an adversary. Which of the following in the MOST likely explanation for why the organization network was compromised?

A. There was a false positive since the network was fully patched.

B. The system administrator did not perform a full system sun.

C. The systems administrator performed a credentialed scan.

D. The vulnerability database was not updated.

Correct Answer: B

QUESTION 4

A security administrator wants to implement two-factor authentication for network switches and routers. The solution should integrate with the company\\'s RADIUS server, which is used for authentication to the network infrastructure devices. The security administrator implements the following:

1.

An HOTP service is installed on the RADIUS server.

2.

The RADIUS server is configured to require the HOTP service for authentication.

The configuration is successfully tested using a software supplicant and enforced across all network devices. Network administrators report they are unable to log onto the network devices because they are not being prompted for the second factor.

Which of the following should be implemented to BEST resolve the issue?

A. Replace the password requirement with the second factor. Network administrators will enter their username and then enter the token in place of their password in the password field.

B. Configure the RADIUS server to accept the second factor appended to the password. Network administrators will enter a password followed by their token in the password field.

C. Reconfigure network devices to prompt for username, password, and a token. Network administrators will enter their username and password, and then they will enter the token.

D. Install a TOTP service on the RADIUS server in addition to the HOTP service. Use the HOTP on older devices that do not support two-factor authentication. Network administrators will use a web portal to log onto these devices.

Correct Answer: B

QUESTION 5

A security administrator is confirming specific ports and IP addresses that are monitored by the IPS- IDS system as well as the firewall placement on the perimeter network between the company and a new business partner Which of the following business documents defines the parameters the security administrator must confirm?

A. BIA

B. ISA

C. NDA

D. MOU

Correct Answer: A