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

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

QUESTION 1

Which of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?

A. Test password complexity of all login fields and input validation of form fields

B. Reverse engineering any thick client software that has been provided for the test

C. Undertaking network-based denial of service attacks in production environment

D. Attempting to perform blind SQL injection and reflected cross-site scripting attacks

E. Running a vulnerability scanning tool to assess network and host weaknesses

Correct Answer: C

Penetration testing is done to look at a network in an adversarial fashion with the aim of looking at what an attacker will use. Penetration testing is done without malice and undertaking a network-based denial of service attack in the production environment is as such `OUT OF SCOPE\\'.

QUESTION 2

The director of sales asked the development team for some small changes to increase the usability of an application used by the sales team. Prior security reviews of the code showed no significant vulnerabilities, and since the changes were small, they were given a peer review and then pushed to the live environment. Subsequent vulnerability scans now show numerous flaws that were not present in the previous versions of the code. Which of the following is an SDLC best practice that should have been followed?

A. Versioning

B. Regression testing

C. Continuous integration

D. Integration testing

Correct Answer: B

QUESTION 3

Which of the following system would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect ... secrecy?

A. Endpoints

B. VPN concentrators

C. Virtual hosts

D. SIEM

E. Layer 2 switches

Correct Answer: B

QUESTION 4

A government contractor was the victim of a malicious attack that resulted in the theft of sensitive information. An analyst\\'s subsequent investigation of sensitive systems led to the following discoveries:

There was no indication of the data owner\\'s or user\\'s accounts being compromised.

No database activity outside of previous baselines was discovered.

All workstations and servers were fully patched for all known vulnerabilities at the time of the attack.

It was likely not an insider threat, as all employees passed polygraph tests.

Given this scenario, which of the following is the MOST likely attack that occurred?

A. The attacker harvested the hashed credentials of an account within the database administrators group after dumping the memory of a compromised machine. With these credentials, the attacker was able to access the database containing sensitive information directly.

B. An account, which belongs to an administrator of virtualization infrastructure, was compromised with a successful phishing attack. The attacker used these credentials to access the virtual machine manager and made a copy of the target virtual machine image. The attacker later accessed the image offline to obtain sensitive information.

C. A shared workstation was physically accessible in a common area of the contractor\\'s office space and was compromised by an attacker using a USB exploit, which resulted in gaining a local administrator account. Using the local administrator credentials, the attacker was able to move laterally to the server hosting the database with sensitive information.

D. After successfully using a watering hole attack to deliver an exploit to a machine, which belongs to an employee of the contractor, an attacker gained access to a corporate laptop. With this access, the attacker then established a remote session over a VPN connection with the server hosting the database of sensitive information.

Correct Answer: C

QUESTION 5

An application developer has been informed of a web application that is susceptible to a clickjacking vulnerability Which of the following code snippets would be MOST applicable to resolve this vulnerability?

A. Content-Security-Policy frame-ancestors: \\'none\\'

B. $escaped_command = escapeshellcmd(Sargs); exec ($escaped_command, Soutput, $return_var);

C. sqlQuery= \\'SELECT * FROM custTable WHERE User=? AND Pass=?\\' parameters.add("User", username)

D. require \\'digest/sha2\\' sha256 = Digest::SHA2.new(256)

Correct Answer: A

Content-Security-Policy: frame-ancestors \\'none';

This prevents any domain from framing the content This setting is recommended unless a specific need has been identified for framing