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.geekcert.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 ISP is receiving reports from a portion of its customers who state that typosquatting is occurring when they type in a portion of the URL for the ISP\\'s website. The reports state that customers are being directed to an advertisement website that is asking for personal information. The security team has verified the DNS system is returning proper results and has no known lOCs. Which of the following should the security team implement to best mitigate this situation?

A. DNSSEC

B. DNS filtering

C. Multifactor authentication

D. Self-signed certificates

E. Revocation of compromised certificates

Correct Answer: B

DNS filtering can be used to prevent users from accessing malicious or unintended websites by blocking certain domains at the DNS level. In the case of typosquatting, where users are being directed to an advertisement website asking for personal information, DNS filtering can help by blocking access to these known malicious domains. This would ensure that even if users mistype a URL, they will not be directed to a harmful site.

QUESTION 2

A security analyst has been tasked with assessing a new API. The analyst needs to be able to test for a variety of different inputs, both malicious and benign, in order to close any vulnerabilities. Which of the following should the analyst use to achieve this goal?

A. Static analysis

B. Input validation

C. Fuzz testing

D. Post-exploitation

Correct Answer: C

Fuzz testing, or fuzzing, is a software testing technique that involves providing invalid, unexpected, or random data as input to a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for potential memory leaks. This type of testing can help identify security vulnerabilities that could be exploited by malicious inputs.

QUESTION 3

A security analyst is reviewing weekly email reports and finds an average of 1.000 emails received daily from the internal security alert email address. Which of the following should be implemented?

A. Tuning the network monitoring service

B. Separation of duties for systems administrators

C. Machine learning algorithms

D. DoS attack prevention

Correct Answer: D

Reference: https://www.mimecast.com/bloq/what-is-dos-attack-and-how-to-Drevent-it/

QUESTION 4

A company is experiencing a large number of attempted network-based attacks against its online store. To determine the best course of action, a security analyst reviews the following logs.

```
10:12:04 192.168.1.1 GET https://comptia.org/products?category='-- 200
10:12:05 192.168.1.1 POST https://comptia.org/products?feedback=%3cscript%3c -- 200
```

Which of the following should the company do NEXT to mitigate the risk of a compromise from these attacks?

A. Restrict HTTP methods.

B. Perform parameterized queries.

C. Implement input sanitization.

D. Validate content types.

Correct Answer: C

QUESTION 5

An attacker infiltrated an electricity-generation site and disabled the safety instrumented system. Ransomware was also deployed on the engineering workstation. The environment has back-to-back firewalls separating the corporate and OT systems. Which of the following is the MOST likely security consequence of this attack?

A. A turbine would overheat and cause physical harm.

B. The engineers would need to go to the historian.

C. The SCADA equipment could not be maintained.

D. Data would be exfiltrated through the data diodes.

Correct Answer: C