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.passapply.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

A MSSP has taken on a large client that has government compliance requirements. Due to the sensitive nature of communications to its aerospace partners, the MSSP must ensure that all communications to and from the client web portal are secured by industry-standard asymmetric encryption methods. Which of the following should the MSSP configure to BEST meet this objective?

A. ChaCha20

B. RSA

C. AES256

D. RIPEMD

Correct Answer: B

QUESTION 2

Ann. a user, brings her laptop to an analyst after noticing it has been operating very slowly. The security analyst examines the laptop and obtains the following output:

```
Active Connections
Proto    Local Address       Foreign Address     State          PID
TCP      0.0.0.0:135         0.0.0.0.0           Listening      513
TCP      0.0.0.0.:445        0.0.0.0.0           Listening      4
TCP      10.11.43.115:139    0.0.0.0.0           Listening      4
TCP      10.11.43.115:65246  208.113.65.18:443   Established    3522
TCP      10.11.43.115:65248  208.113.65.18:443   Established    3522
```

Which of the following will the analyst most likely use NEXT?

A. Process explorer

B. Vulnerability scanner

C. Antivirus

D. Network enumerator

Correct Answer: B

QUESTION 3

An organization collects personal data from its global customers. The organization determines how that data is going to be used, why it is going to be used, and how it is manipulated for business processes. Which of the following will the organization need in order to comply with GDPR? (Choose two.)

A. Data processor

B. Data custodian

C. Data owner

D. Data steward

E. Data controller

F. Data manager

Correct Answer: AE

QUESTION 4

A security operations center analyst is investigating anomalous activity between a database server and an unknown external IP address and gathered the following data:

dbadmin last logged in at 7:30 a.m. and logged out at 8:05 a.m. A persistent TCP/6667 connection to the external address was established at 7:55 a.m.

The connection is still active.

Other than bytes transferred to keep the connection alive, only a few kilobytes of data transfer every hour since the start of the connection.

A sample outbound request payload from PCAP showed the ASCII content:";JOIN #community".

Which of the following is the MOST likely root cause?

A. A SQL injection was used to exfiltrate data from the database server.

B. The system has been hijacked for cryptocurrency mining.

C. A botnet Trojan is installed on the database server.

D. The dbadmin user is consulting the community for help via Internet Relay Chat.

Correct Answer: C

QUESTION 5

A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an except of output from the troubleshooting session:

```
openssl s_client -host ldap1.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=danville/CN=chicago
```

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

A. The clients may not trust idapt by default.

B. The secure LDAP service is not started, so no connections can be made.

C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.

D. Secure LDAP should be running on UDP rather than TCP.

E. The company is using the wrong port. It should be using port 389 for secure LDAP.

F. Secure LDAP does not support wildcard certificates.

G. The clients may not trust Chicago by default.

Correct Answer: BE