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.certbus.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 social media company wants to change encryption ciphers after identifying weaknesses in the implementation of the existing ciphers. The company needs the new ciphers to meet the following requirements:

? Utilize less RAM than competing ciphers.

? Be more CPU-efficient than previous ciphers.

? Require customers to use TLS 1.3 while broadcasting video or audio.

Which of the following is the best choice for the social media company?

A. IDEA-CBC

B. AES-GCM

C. ChaCha20-Poly1305

D. Camellia-CBC

Correct Answer: C

QUESTION 2

A security manager wants to implement a policy that will management with the ability to monitor employees\\' activities with minimum impact to productivity. Which of the following policies Is BEST suited for this scenario?

A. Separation of duties

B. Mandatory vacations

C. Least privilege

D. Incident response

Correct Answer: A

QUESTION 3

A major broadcasting company that requires continuous availability to streaming content needs to be resilient against DDoS attacks. Which of the following Is the MOST important infrastructure security design element to prevent an outage?

A. Supporting heterogeneous architecture

B. Leveraging content delivery network across multiple regions

C. Ensuring cloud autoscaling is in place

D. Scaling horizontally to handle increases in traffic

Correct Answer: B

QUESTION 4

A security analyst is reviewing a new IOC in which data is injected into an online process. The IOC shows the data injection could happen in the following ways:

1.

Five numerical digits followed by a dash, followed by four numerical digits; or

2.

Five numerical digits

When one of these IOCs is identified, the online process stops working. Which of the following regular expressions should be implemented in the NIPS?

A. ^\d{4}(-\d{5})?$

B. ^\d{5}(-\d{4})?$

C. ^\d{5-4}$

D. ^\d{9}$

Correct Answer: B

QUESTION 5

An organization is designing a network architecture that must meet the following requirements:

1.

Users will only be able to access predefined services.

2.

Each user will have a unique allow list defined for access.

3.

The system will construct one-to-one subject/object access paths dynamically.

Which of the following architectural designs should the organization use to meet these requirements?

A. Peer-to-peer secure communications enabled by mobile applications

B. Proxied application data connections enabled by API gateways

C. Microsegmentation enabled by software-defined networking

D. VLANs enabled by network infrastructure devices

Correct Answer: C

QUESTION 6

In a cloud environment, the provider offers relief to an organization\\'s teams by sharing in many of the operational duties. In a shared responsibility model, which of the following responsibilities belongs to the provider in a PaaS implementation?

A. Application-specific data assets

B. Application user access management

C. Application-specific logic and code

D. Application/platform software

Correct Answer: D

QUESTION 7

A network administrator who manages a Linux web server notices the following traffic:

http://comptia.org/../../../../etc/shadow

Which of the following is the BEST action for the network administrator to take to defend against this type of web attack?

A. Validate the server certificate and trust chain.

B. Validate the server input and append the input to the base directory path.

C. Validate that the server is not deployed with default account credentials.

D. Validate that multifactor authentication is enabled on the server for all user accounts.

Correct Answer: B

QUESTION 8

A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client\\'s systems?

A. The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.

B. The change control board must review and approve a submission.

C. The information system security officer provides the systems engineer with the system updates.

D. The security engineer asks the project manager to review the updates for the client\\'s system.

Correct Answer: B

QUESTION 9

A cyberanalyst for a government agency is concerned about how Pll is protected A supervisor indicates that a Privacy Impact Assessment must be done. Which of the following describes a function of a Privacy Impact Assessment?

A. To validate the project participants

B. To identify the network ports

C. To document residual risks

D. To evaluate threat acceptance

Correct Answer: C

A Privacy Impact Assessment (PIA) is a process used to evaluate and manage privacy risks associated with the collection, use, and storage of personally identifiable information (PII). One of the key functions of a PIA is to document residual risks, which are the privacy risks that remain after controls have been applied. By identifying and documenting these risks, organizations can make informed decisions about whether additional measures are needed or whether certain risks are acceptable.

QUESTION 10

A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.

The technician will define this threat as:

A. a decrypting RSA using obsolete and weakened encryption attack.

B. a zero-day attack.

C. an advanced persistent threat.

D. an on-path attack.

Correct Answer: C

Reference: https://www.internetsociety.org/deploy360/tls/basics/

QUESTION 11

The information security manager at a 24-hour manufacturing facility is reviewing a contract for potential risks to the organization. The contract pertains to the support of printers and multifunction devices during non-standard business hours. Which of the following will the security manager most likely identify as a risk?

A. Print configurations settings for locked print jobs

B. The lack of an NDA with the company that supports its devices

C. The lack of an MSA to govern other services provided by the service provider

D. The lack of chain of custody for devices prior to deployment at the company

Correct Answer: B

A non-disclosure agreement (NDA) is crucial when external parties are provided access to sensitive company devices or information. The absence of an NDA poses a risk that confidential information could be disclosed by the service provider. Therefore, ensuring an NDA is in place with the company that supports sensitive devices would be a key risk identified in the contract.

QUESTION 12

A security engineer is reviewing a record of events after a recent data breach incident that Involved the following:

1.

A hacker conducted reconnaissance and developed a footprint of the company s Internet- facing web application assets.

2.

A vulnerability in a third-party horary was exploited by the hacker, resulting in the compromise of a local account.

3.

The hacker took advantage of the account\\'s excessive privileges to access a data store and exfilltrate the data without detection.

Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis

B. Secure web gateway

C. Software composition analysis

D. User behavior analysis

E. Web application firewall

Correct Answer: C

QUESTION 13

A security engineer investigates an incident and determines that a rogue device is on the network. Further investigation finds that an employee\\'s personal device has been set up to access company resources and does not comply with standard security controls. Which of the following should the security engineer recommend to reduce the risk of future reoccurrence?

A. Require device certificates to access company resources.

B. Enable MFA at the organization\\'s SSO portal.

C. Encrypt all workstation hard drives.

D. Hide the company wireless SSID.

Correct Answer: A

To reduce the risk of unauthorized devices accessing company resources, requiring device certificates is an effective control. Device certificates can be used to authenticate devices before they are allowed to connect to the network and access resources, ensuring that only devices with a valid certificate, which are typically managed and issued by the organization, can connect.

QUESTION 14

A pharmaceutical company uses a cloud provider to host thousands of independent resources in object storage. The company needs a practical and effective means of discovering data, monitoring changes, and identifying suspicious activity. Which of the following would best meet these requirements?

A. A machine-learning-based data security service

B. A file integrity monitoring service

C. A cloud configuration assessment and compliance service

D. A cloud access security broker

Correct Answer: D

QUESTION 15

The Chief Information Security Officer (CISO) is working with a new company and needs a legal document to ensure all parties understand their roles during an assessment. Which of the following should the CISO have each party sign?

A. SLA

B. ISA

C. Permissions and access

D. Rules of engagement

Correct Answer: D

The Rules of Engagement (ROE) document is essential for ensuring all parties understand their roles, responsibilities, and limitations during an assessment. It provides a clear framework that helps prevent legal and operational misunderstandings, making it the most appropriate choice for the CISO to have each party sign in this scenario.