- **Vendor:** CompTIA
- **Exam Code:** CAS-004
- **Exam Name:** CompTIA Advanced Security Practitioner (CASP+)
- **New Updated Questions from Braindump2go**
- **(Updated in April/2024)**

QUESTION 573
A small bank is evaluating different methods to address and resolve the following requirements:
- Must be able to store credit card data using the smallest amount of data possible.
- Must be compliant with PCI DSS.
- Must maintain confidentiality if one piece of the layer is compromised.

Which of the following is the BEST solution for the bank?

A. Scrubbing
B. Tokenization
C. Masking
D. Homomorphic encryption

Answer: B

QUESTION 574
When implementing serverless computing, an organization must still account for:

A. the underlying computing network infrastructure.
B. hardware compatibility.
C. the security of its data.
D. patching the service.

Answer: C

QUESTION 575
A systems administrator at a web-hosting provider has been tasked with renewing the public certificates of all customer sites. Which of the following would BEST support multiple domain names while minimizing the amount of certificates needed?

A. OCSP
B. CRL
C. SAN
D. CA

Answer: C

QUESTION 576

An IT department is currently working to implement an enterprise DLP solution. Due diligence and best practices must be followed in regard to mitigating risk. Which of the following ensures that authorized modifications are well planned and executed?

A. Risk management
B. Network management
C. Configuration management
D. Change management

Answer: D

QUESTION 577
A company's Chief Information Security Officer wants to prevent the company from being the target of ransomware. The company's IT assets need to be protected. Which of the following are the MOST secure options to address these concerns? (Choose three.)

A. Antivirus
B. EDR
C. Sandboxing
D. Application control
E. Host-based firewall
F. IDS
G. NGFW
H. Strong authentication

Answer: CDG

QUESTION 578
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

Answer: C

QUESTION 579
An online video shows a company's Chief Executive Officer (CEO) making a company announcement. The CEO, however, did not make the announcement. Which of the following BEST describes this attack?

A. Identity theft
B. Deepfake
C. Website defacement
D. Social engineering

Answer: B

QUESTION 580
A security engineer needs to implement a cost-effective authentication scheme for a new web-based application that requires:
- Rapid authentication
- Flexible authorization

- Ease of deployment
- Low cost but high functionality

Which of the following approaches best meets these objectives?

A. Kerberos
B. EAP
C. SAML
D. OAuth
E. TACACS+

Answer: D

QUESTION 581
Which of the following technologies would benefit the most from the use of biometric readers, proximity badge entry systems, and the use of hardware security tokens to access various environments and data entry systems?

A. Deep learning
B. Machine learning
C. Nanotechnology
D. Passwordless authentication
E. Biometric impersonation

Answer: D

QUESTION 582
A hospital has fallen behind with patching known vulnerabilities due to concerns that patches may cause disruptions in the availability of data and impact patient care. The hospital does not have a tracking solution in place to audit whether systems have been updated or to track the length of time between notification of the weakness and patch completion. Since tracking is not in place, the hospital lacks accountability with regard to who is responsible for these activities and the timeline of patching efforts. Which of the following should the hospital do first to mitigate this risk?

A. Complete a vulnerability analysis.
B. Obtain guidance from the health ISAC.
C. Purchase a ticketing system for auditing efforts.
D. Ensure CVEs are current.
E. Train administrators on why patching is important.

Answer: C

QUESTION 583
The Chief Executive Officer of an online retailer notices a sudden drop in sales. A security analyst at the retailer detects a redirection of unsecure web traffic to a competitor's site. Which of the following would best prevent this type of attack?

A. Enabling HSTS
B. Configuring certificate pinning
C. Enforcing DNSSEC
D. Deploying certificate stapling

Answer: A

QUESTION 584
A security administrator is trying to securely provide public access to specific data from a web application. Clients who want to access the application will be required to:
- Only allow the POST and GET options.
- Transmit all data secured with TLS 1.2 or greater.

- Use specific URLs to access each type of data that is requested.
- Authenticate with a bearer token.

Which of the following should the security administrator recommend to meet these requirements?

A. API gateway
B. Application load balancer
C. Web application firewall
D. Reverse proxy

Answer: A

QUESTION 585
An organization established an agreement with a partner company for specialized help desk services. A senior security officer within the organization is tasked with providing documentation required to set up a dedicated VPN between the two entities. Which of the following should be required?

A. SLA
B. ISA
C. NDA
D. MOU

Answer: B

QUESTION 586
During a network defense engagement, a red team is able to edit the following registry key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
Which of the following tools is the red team using to perform this action?

A. PowerShell
B. SCAP scanner
C. Network vulnerability scanner
D. Fuzzer

Answer: A

QUESTION 587
An IoT device implements an encryption module built within its SoC, where the asymmetric private key has been defined in a write-once read-many portion of the SoC hardware. Which of the following should the IoT manufacture do if the private key is compromised?

A. Use over-the-air updates to replace the private key.
B. Manufacture a new IoT device with a redesigned SoC.
C. Replace the public portion of the IoT key on its servers.
D. Release a patch for the SoC software.

Answer: B

QUESTION 588
Which of the following is record-level encryption commonly used to do?

A. Protect database fields.
B. Protect individual files.
C. Encrypt individual packets.
D. Encrypt the master boot record.

Answer: A

QUESTION 589
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 IOCs. 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

Answer: A

QUESTION 590
A cloud security engineer is setting up a cloud-hosted WAF. The engineer needs to implement a solution to protect the multiple websites the organization hosts. The organization websites are:
- `www.mycompany.org`
- `www.mycompany.com`
- `campus.mycompany.com`
- `wiki.mycompany.org`

The solution must save costs and be able to protect all websites. Users should be able to notify the cloud security engineer of any on-path attacks. Which of the following is the best solution?

A. Purchase one SAN certificate.
B. Implement self-signed certificates.
C. Purchase one certificate for each website.
D. Purchase one wildcard certificate.

Answer: D

QUESTION 591
A partner organization is requesting that a security administrator exchange S/MIME certificates for email between the two organizations. The partner organization is most likely trying to:

A. utilize digital signatures to ensure data integrity.
B. reduce the amount of impersonation spam the organization receives.
C. enable a more decentralized IT infrastructure.
D. eliminate the organization's business email compromise risks.

Answer: A

QUESTION 592
The general counsel at an organization has received written notice of upcoming litigation. The general counsel has issued a legal records hold. Which of the following actions should the organization take to comply with the request?

A. Preserve all communication matching the requested search terms.
B. Block communication with the customer while litigation is ongoing.
C. Require employees to be trained on legal record holds.
D. Request that all users do not delete any files.

Answer: A

QUESTION 593
An organization recently completed a security controls assessment. The results highlighted the following vulnerabilities:
- Out-of-date definitions
- Misconfigured operating systems
- An inability to detect active attacks
- Unimpeded access to critical servers' USB ports

Which of the following will most likely reduce the risks that were identified by the assessment team?

A. Install EDR on endpoints, configure group policy, lock server room doors, and install a camera system with guards watching 24/7.
B. Create an information security program that addresses user training, perform weekly audits of user workstations, and utilize a centralized configuration management program.
C. Update antivirus definitions, install NGFW with logging enabled, use USB port lockers, and run SCAP scans weekly.
D. Implement a vulnerability management program and a SIEM tool with alerting, install a badge system with zones, and restrict privileged access.

Answer: C

QUESTION 594
A penetration tester discovers a condition that causes unexpected behavior in a web application. This results in the dump of the interpreter's debugging information, which includes the interpreter's version, full path of binary files, and the user ID running the process. Which of the following actions would best mitigate this risk?

A. Include routines in the application for message handling.
B. Adopt a compiled programming language instead.
C. Perform SAST vulnerability scans on every build.
D. Validate user-generated input.

Answer: B

QUESTION 595
A company with multiple locations has taken a cloud-only approach to its infrastructure. The company does not have standard vendors or systems, resulting in a mix of various solutions put in place by each location. The Chief Information Security Officer wants to ensure that the internal security team has visibility into all platforms. Which of the following best meets this objective?

A. Security information and event management
B. Cloud security posture management
C. SNMPv2 monitoring and log aggregation
D. Managed detection and response services from a third party

Answer: B

QUESTION 596
A cyberanalyst for a government agency is concerned about how PII 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

Answer: C

QUESTION 597

A Chief Information Security Officer (CISO) reviewed data from a cyber exercise that examined all aspects of the company's response plan. Which of the following best describes what the CISO reviewed?

A. An after-action report
B. A tabletop exercise
C. A system security plan
D. A disaster recovery plan

Answer: A

QUESTION 598
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

Answer: D

QUESTION 599
A multinational organization was hacked, and the incident response team's timely action prevented a major disaster. Following the event, the team created an after action report. Which of the following is the primary goal of an after action review?

A. To gather evidence for subsequent legal action
B. To determine the identity of the attacker
C. To identify ways to improve the response process
D. To create a plan of action and milestones

Answer: C

QUESTION 600
A security engineer needs to select the architecture for a cloud database that will protect an organization's sensitive data. The engineer has a choice between a single-tenant or a multitenant database architecture offered by a cloud vendor. Which of the following best describes the security benefits of the single-tenant option? (Choose two.)

A. Most cost-effective
B. Ease of backup and restoration
C. High degree of privacy
D. Low resilience to side-channel attacks
E. Full control and ability to customize
F. Increased geographic diversity

Answer: CE