Vendor: CompTIA

Exam Code: CAS-004

Exam Name: CompTIA Advanced Security Practitioner (CASP+) Exam

Version: 13.02

Q & As: 180

QUESTION 1
A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs. Which of the following should the company use to prevent data theft?

A. Watermarking
B. DRM
C. NDA
D. Access logging

Correct Answer: A

QUESTION 2
A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals. Which of the following does the business's IT manager need to consider?

A. The availability of personal data
B. The right to personal data erasure
C. The company's annual revenue
D. The language of the web application

Correct Answer: B

QUESTION 3
A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:

▪ Must have a minimum of 15 characters
▪ Must use one number
▪ Must use one capital letter
▪ Must not be one of the last 12 passwords used

Which of the following policies should be added to provide additional security?

A. Shared accounts
B. Password complexity
C. Account lockout
D. Password history
E. Time-based logins

Correct Answer: C

QUESTION 4
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location. Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

A. Execute never
B. No-execute
C. Total memory encryption
D. Virtual memory encryption

Correct Answer: B

QUESTION 5
A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks. Which of the following would be the BEST solution against this type of attack?

A. Cookies
B. Wildcard certificates
C. HSTS
D. Certificate pinning

Correct Answer: D

QUESTION 6
Which of the following agreements includes no penalties and can be signed by two entities that are working together toward the same goal?

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

Correct Answer: A

QUESTION 7
A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident. Which of the following would be BEST to proceed with the transformation?

A. An on-premises solution as a backup
B. A load balancer with a round-robin configuration
C. A multicloud provider solution
D. An active-active solution within the same tenant

Correct Answer: C

QUESTION 8
A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise. The company would like to find a way to use this information to protect the environment while still gaining valuable attack information. Which of the following would be BEST for the company to implement?

A. A WAF
B. An IDS
C. A SIEM
D. A honeypot

Correct Answer: D

QUESTION 9
A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic. Which of the following would satisfy the requirement?

A. NIDS
B. NIPS
C. WAF
D. Reverse proxy

Correct Answer: A

QUESTION 10
A security is assisting the marketing department with ensuring the security of the organization's social media platforms. The two main concerns are:

▪ The Chief marketing officer (CMO) email is being used department wide as the username
▪ The password has been shared within the department

Which of the following controls would be BEST for the analyst to recommend?

A. Configure MFA for all users to decrease their reliance on other authentication.
B. Have periodic, scheduled reviews to determine which OAuth configuration are set for each media platform.
C. Create multiple social media accounts for all marketing user to separate their actions.
D. Ensue the password being shared is sufficiently and not written down anywhere.

Correct Answer: A

QUESTION 11
A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

```
High (CVSS: 10.0)
NVT: PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)  (OID: 1.3.6.1.4.1.25623.1.0.803317)
Product detection result: cpe:/a:php:php:5.3.6 by PHP Version Detection (Remote)  (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to buffer overflow vulnerability.
Vulnerability Detection ResultInstalled version: 5.3.6
Fixed version: 5.3.15/5.4.5

Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions. Impact Level: System/Application
```

Which of the following MOST appropriate corrective action to document for this finding?

A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
C. The system administrator should evaluate dependencies and perform upgrade as necessary.
D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

Correct Answer: A

QUESTION 12