CompTIA

CAS-003 Exam

CompTIA Advanced Security Practitioner (CASP) Exam

Questions & Answers
(Demo Version – Limited Content)

Thank you for Downloading CAS-003 exam PDF Demo

Version: 23.0

Question: 1

An organization is implementing a virtualized thin-client solution for normal user computing and access. During a review of the architecture, concerns were raised that an attacker could gain access to multiple user environments by simply gaining a foothold on a single one with malware. Which of the following reasons BEST explains this?

A. Malware on one virtual environment could enable pivoting to others by leveraging vulnerabilities in the hypervisor.
B. A worm on one virtual environment could spread to others by taking advantage of guest OS networking services vulnerabilities.
C. One virtual environment may have one or more application-layer vulnerabilities, which could allow an attacker to escape that environment.
D. Malware on one virtual user environment could be copied to all others by the attached network storage controller.

Answer: A

Question: 2

An online bank has contracted with a consultant to perform a security assessment of the bank's web portal. The consultant notices the login page is linked from the main page with HTTPS, but when the URL is changed to HTTP, the browser is automatically redirected back to the HTTPS site. Which of the following is a concern for the consultant, and how can it be mitigated?

A. XSS could be used to inject code into the login page during the redirect to the HTTPS site. The consultant should implement a WAF to prevent this.
B. The consultant is concerned the site is using an older version of the SSL 3.0 protocol that is vulnerable to a variety of attacks. Upgrading the site to TLS 1.0 would mitigate this issue.
C. The HTTP traffic is vulnerable to network sniffing, which could disclose usernames and passwords to an attacker. The consultant should recommend disabling HTTP on the web server.
D. A successful MITM attack Could intercept the redirect and use sslstrip to decrypt further HTTPS traffic. Implementing HSTS on the web server would prevent this.

Answer: D

Question: 3

A security administrator wants to implement controls to harden company-owned mobile devices. Company policy specifies the following requirements:
Mandatory access control must be enforced by the OS.
Devices must only use the mobile carrier data transport.
Which of the following controls should the security administrator implement? (Select three).

A. Enable DLP
B. Enable SEAndroid
C. Enable EDR
D. Enable secure boot
E. Enable remote wipe
F. Disable Bluetooth
G. Disable 802.11
H. Disable geotagging

Answer: B,F,G

Question: 4

While conducting online research about a company to prepare for an upcoming penetration test, a security analyst discovers detailed financial information on an investor website the company did not make public. The analyst shares this information with the Chief Financial Officer (CFO), who confirms the information is accurate, as it was recently discussed at a board of directors meeting. Many of the details are verbatim discussion comments captured by the board secretary for purposes of transcription on a mobile device. Which of the following would MOST likely prevent a similar breach in the future?

A. Remote wipe
B. FDE
C. Geolocation
D. eFuse
E. VPN

Answer: B

Question: 5

DRAG DROP
Drag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all.

Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	
Collection of organizations in the same industry vertical developing services based on a common application stack	
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	
Marketing organization that outsources email delivery to An online provider	
Organization that has migrated their highly customized external websites into the cloud	

Community cloud with IaaS

Community cloud with PaaS

Community cloud with SaaS

Hybrid cloud

Private cloud with IaaS

Private cloud with PaaS

Private cloud with SaaS

Public cloud with IaaS

Public cloud with PaaS

Public cloud with SaaS

Answer:

Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	Private cloud with IaaS
Collection of organizations in the same industry vertical developing services based on a common application stack	Community cloud with PaaS
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	Hybrid cloud
Marketing organization that outsources email delivery to An online provider	Public cloud with SaaS
Organization that has migrated their highly customized external websites into the cloud	Public cloud with PaaS

Community cloud with IaaS | Community cloud with PaaS | Community cloud with SaaS | Hybrid cloud

Private cloud with IaaS | Private cloud with PaaS | Private cloud with SaaS | Public cloud with IaaS

Public cloud with PaaS | Public cloud with SaaS

Question: 6

An infrastructure team within an energy organization is at the end of a procurement process and has selected a vendor's SaaS platform to deliver services. As part of the legal negotiation, there are a number of outstanding risks, including:

There are clauses that confirm a data retention period in line with what is in the energy organization's security policy.

The data will be hosted and managed outside of the energy organization's geographical location.

The number of users accessing the system will be small, and no sensitive data will be hosted in the SaaS platform. Which of the following should the project's security consultant recommend as the

NEXT step?

A. Develop a security exemption, as the solution does not meet the security policies of the energy organization.
B. Require a solution owner within the energy organization to accept the identified risks and consequences.
C. Mititgate the risks by asking the vendor to accept the in-country privacy principles and modify the retention period.
D. Review the procurement process to determine the lessons learned in relation to discovering risks toward the end of the process.

Answer: B

Question: 7

A developer emails the following output to a security administrator for review:

```
curl -X TRACE host1
User-Agent: curl/7.25.0
Host: host1
Accept: */*
Cookie: user=badguy: path=/; HttpOnly
```

Which of the following tools might the security administrator use to perform further security assessment of this issue?

A. Port scanner
B. Vulnerability scanner
C. Fuzzer
D. HTTP interceptor

Answer: D

Question: 8

A software development company lost customers recently because of a large number of software issues. These issues were related to integrity and availability defects, including buffer overflows, pointer deferences, and others. Which of the following should the company implement to improve code quality? (Select two).

A. Development environment access controls
B. Continuous integration
C. Code comments and documentation
D. Static analysis tools
E. Application containerization
F. Code obfuscation

Answer: D,F

Question: 9

An enterprise is trying to secure a specific web-based application by forcing the use of multifactor authentication. Currently, the enterprise cannot change the application's sign-in page to include an extra field. However, the web-based application supports SAML. Which of the following would BEST secure the application?

A. Using an SSO application that supports mutlifactor authentication
B. Enabling the web application to support LDAP integration
C. Forcing higher-complexity passwords and frequent changes
D. Deploying Shibboleth to all web-based applications in the enterprise

Answer: D

Question: 10

After significant vulnerabilities and misconfigurations were found in numerous production web applications, a security manager identified the need to implement better development controls. Which of the following controls should be verified? (Select two).

A. Input validation routines are enforced on the server side.
B. Operating systems do not permit null sessions.
C. Systems administrators receive application security training.
D. VPN connections are terminated after a defined period of time.
E. Error-handling logic fails securely.
F. OCSP calls are handled effectively.

Answer: A,E

Thank You for trying CAS-003 PDF Demo

Start Your CAS-003 Preparation