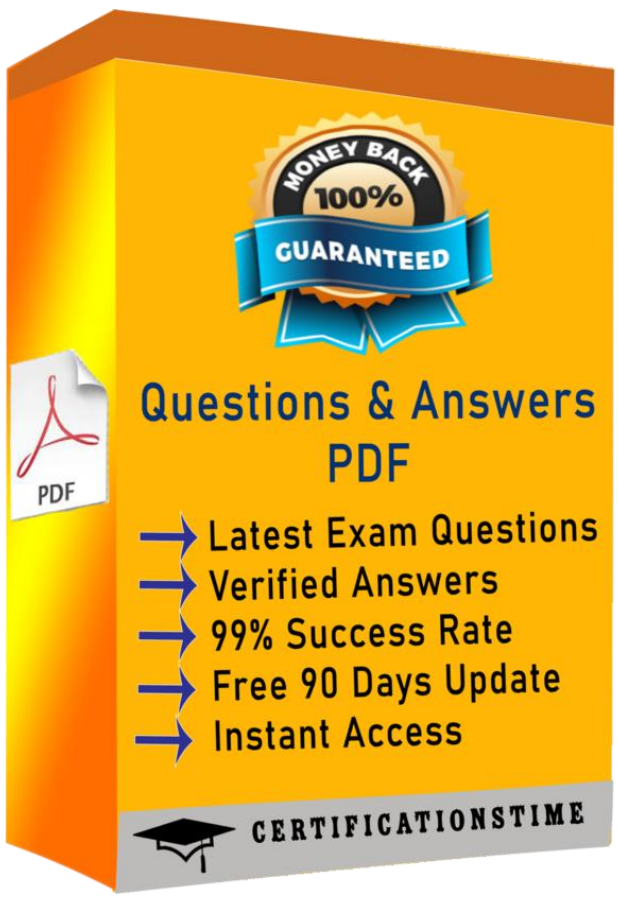
CompTIA
CAS-003

CompTIA Advanced Security Practitioner (CASP)

https://certificationstime.com/



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

An organization wants to allow its employees to receive corporate email on their own smartphones.
A security analyst is reviewing the following information contained within the file system of an employee's smartphone:
FamilyPix.jpg
Taxreturn.tax
paystub.pdf
employeesinfo.xls
SoccerSchedule.doc
RecruitmentPlan.xls
Based on the above findings, which of the following should the organization implement to prevent further exposure? (Select two).
A. Remote wiping
B. Side loading
C. VPN
D. Containerization
E. Rooting
F. Geofencing
G. Jailbreaking
Answer: A,C

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