Exam : **CAS-003**

Title : CompTIA Advanced Security Practitioner (CASP)

Version : DEMO

1.The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company.
A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:
A. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controls
B. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awareness
C. corporate general counsel requires a single system boundary to determine overall corporate risk exposure
D. major risks identified by the subcommittee merit the prioritized allocation of scare funding to address cybersecurity concerns
Answer: A

2.A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems.
The security architect has identified the following requirements:
1. Information should be sourced from the trusted master data source.
2. There must be future requirements for identity proofing of devices and users.
3. A generic identity connector that can be reused must be developed.
4. The current project scope is for internally hosted applications only.
Which of the following solution building blocks should the security architect use to BEST meet the requirements?
A. LDAP, multifactor authentication, oAuth, XACML
B. AD, certificate-based authentication, Kerberos, SPML
C. SAML, context-aware authentication, oAuth, WAYF
D. NAC, radius, 802.1x, centralized active directory
Answer: A

3.A software development team has spent the last 18 months developing a new web-based front-end that will allow clients to check the status of their orders as they proceed through manufacturing. The marketing team schedules a launch party to present the new application to the client base in two weeks. Before the launch, the security team discovers numerous flaws that may introduce dangerous vulnerabilities, allowing direct access to a database used by manufacturing. The development team did not plan to remediate these vulnerabilities during development.
Which of the following SDLC best practices should the development team have followed?
A. Implementing regression testing
B. Completing user acceptance testing
C. Verifying system design documentation
D. Using a SRTM
Answer: D

4.An organization’s Chief Financial Officer (CFO) was the target of several different social engineering

attacks recently. The CFO has subsequently worked closely with the Chief Information Security Officer (CISO) to increase awareness of what attacks may look like. An unexpected email arrives in the CFO's inbox from a familiar name with an attachment.
Which of the following should the CISO task a security analyst with to determine whether or not the attachment is safe?
A. Place it in a malware sandbox.
B. Perform a code review of the attachment.
C. Conduct a memory dump of the CFO's PC.
D. Run a vulnerability scan on the email server.
Answer: A

5.A company has decided to lower costs by conducting an internal assessment on specific devices and various internal and external subnets. The assessment will be done during regular office hours, but it must not affect any production servers.
Which of the following would MOST likely be used to complete the assessment? (Select two.)
A. Agent-based vulnerability scan
B. Black-box penetration testing
C. Configuration review
D. Social engineering
E. Malware sandboxing
F. Tabletop exercise
Answer: A,C