IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **CAS-003**

Title : CompTIA Advanced Security Practitioner (CASP)

Version : DEMO

1.A security engineer must establish a method to assess compliance with company security policies as they apply to the unique configuration of individual endpoints, as well as to the shared configuration policies of common devices.

Policy	Device Type	% of Devices Compliant
Local Administration Accounts Renamed	Server	65%
Guest Account Disabled	Host	30%
Local Firewall Enabled	Host	80%
Password Complexity Enabled	Server	46%

Which of the following tools is the security engineer using to produce the above output?
A. Vulnerability scanner
B. SIEM
C. Port scanner
D. SCAP scanner
Answer: B

2.A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.
Which of the following exercise types should the analyst perform?
A. Summarize the most recently disclosed vulnerabilities.
B. Research industry best practices and latest RFCs.
C. Undertake an external vulnerability scan and penetration test.
D. Conduct a threat modeling exercise.
Answer: D

3.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

4.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

5.A development team is testing an in-house-developed application for bugs. During the test, the application crashes several times due to null pointer exceptions.
Which of the following tools, if integrated into an IDE during coding, would identify these bugs routinely?
A. Issue tracker
B. Static code analyzer
C. Source code repository
D. Fuzzing utility
Answer: D