CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

1. A newly-appointed risk management director for the IT department at Company XYZ, a major pharmaceutical manufacturer, needs to conduct a risk analysis regarding a new system which the developers plan to bring on-line in three weeks. The director begins by reviewing the thorough and well-written report from the independent contractor who performed a security assessment of the system.

A. An incident response plan which guarantees response by tier two support within 15 minutes of an incident.

B. A definitive plan of action and milestones which lays out resolutions to all vulnerabilities within six months.

C. Business insurance to transfer all risk from the company shareholders to the insurance company.

D. A prudent plan of action which details how to decommission the system within 90 days of becoming operational.

Answer(s): B

---

2. A large organization has recently suffered a massive credit card breach. During the months of Incident

A. During the Identification Phase

B. During the Lessons Learned phase

C. During the Containment Phase

D. During the Preparation Phase

Answer(s): B

---

3. The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and wants to connect it to the company's internal network. The Chief Information Security Officer (CISO) was told to research and recommend how to secure this device. Which of the following recommendations should be implemented to keep the device from posing a security risk to the company?

A. A password or PIN to access the device and a corporate policy to prevent sensitive information from residing on a mobile device.

B. Encryption of the non-volatile memory and a password or Pl N to access the device.

C. Encryption of the non-volatile memory and a corporate policy to prevent sensitive information from residing on a mobile device.

D. A corporate policy to prevent sensitive information from residing on a mobile device and antivirus software.

Answer(s): B

---

4. A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

A. Code review

B. Penetration testing

C. Grey box testing

D. Code signing

E. White box testing

Answer(s): A,E

---

5. A system administrator needs to meet the maximum amount of security goals for a new DNS infrastructure. The administrator deploys DNSSEC extensions to the domain names and infrastructure.

A. Availability

B. Authentication

C. Integrity

D. Confidentiality

E. Encryption

Answer(s): B,C

---

6. A new web based application has been developed and deployed in production. A security engineer decides to use an HTTP interceptor for testing the application. Which of the following problems would

A. The tool could show that input validation was only enabled on the client side

B. The tool could enumerate backend SQL database table and column names

C. The tool could force HTTP methods such as DELETE that the server has denied

D. The tool could fuzz the application to determine where memory leaks occur

Answer(s): A

---

7. After a security incident, an administrator would like to implement policies that would help reduce fraud and the potential for collusion between employees. Which of the following would help meet these goals by having co-workers occasionally audit another worker's position?

A. Least privilege

B. Job rotation

C. Mandatory vacation

D. Separation of duties

Answer(s): B

---

8. A trust relationship has been established between two organizations with web based services. One organization is acting as the Requesting Authority (RA) and the other acts as the Provisioning Service

A. The trust relationship uses SPML in the SOAP header. The SOAP body transports the SAML requests/responses.

B. The trust relationship uses SPML in the SAML header. The SAML body transports the SPML requests/ responses.

C. The trust relationship uses XACML in the SAML header. The SAML body transports the SOAP requests/ responses.

D. The trust relationship uses SAML in the SOAP header. The SOAP body transports the SPML requests/ responses.

Answer(s): D

---

9. An IT manager is concerned about the cost of implementing a web filtering solution in an effort to mitigate the risks associated with malware and resulting data leakage. Given that the ARO is twice per year, the

A. $0

B. $7,500

C. $10,000

D. $12,500

E. $15,000

Answer(s): B

---

10. The internal audit department is investigating a possible breach of security. One of the auditors is sent to interview the following employees:

A. The manager should only be able to review the data and approve purchase orders.

B. All employees should have the same access level to be able to check on each others.

C. The manager should be able to both enter and approve information.

D. Employee A and Employee B should rotate jobs at a set interval and cross-train.

Answer(s): A

---

11. A security administrator is assessing a new application. The application uses an API that is supposed to encrypt text strings that are stored in memory. How might the administrator test that the strings are indeed encrypted in memory?

A. Use fuzzing techniques to examine application inputs

B. Run nmap to attach to application memory

C. Use a packet analyzer to inspect the strings

D. Initiate a core dump of the application

E. Use an HTIP interceptor to capture the text strings

Answer(s): D

---

12. A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines.

A. vTPM

B. HSM

C. TPM

D. INE

Answer(s): A

---

13. An organization would like to allow employees to use their network username and password to access a third-party service. The company is using Active Directory Federated Services for their directory service.

A. LDAP/S

B. SAML

C. NTLM

D. OAUTH

E. Kerberos

Answer(s): B,E

---

14. An organization is selecting a Saas provider to replace its legacy, in house Customer Resource

A. Ensure the Saas provider supports dual factor authentication.

B. Ensure the Saas provider supports encrypted password transmission and storage.

C. Ensure the Saas provider supports secure hash file exchange.

D. Ensure the Saas provider supports role-based access control.

E. Ensure the Saas provider supports directory services federation.

Answer(s): E

---

15. A health service provider is considering the impact of allowing doctors and nurses access to the internal email system from their personal smartphones. The Information Security Officer (ISO) has received a technical document from the security administrator explaining that the current email system is capable of enforcing security policies to personal smartphones, including screen lockout and mandatory PINs.

A. Smartphones may be used as rogue access points.

B. Not all smartphones natively support encryption.

C. Smartphone radios can interfere with health equipment.

D. Compliance may not be supported by all smartphones.

E. Equipment loss, theft, and data leakage.

F. Data usage cost could significantly increase.

G. The email system may become unavailable due to overload.

Answer(s): B,D,E

---

16. The element in SAML can be provided in which of the following predefined formats? (Select

A. PTR DNS record

B. WWN record name

C. EV certificate OID extension

D. Kerberos principal name

E. X.509 subject name

Answer(s): D,E

---

17. An enterprise must ensure that all devices that connect to its networks have been previously approved.

A. Implementing federated network access with the third party.

B. Using a HSM at the network perimeter to handle network device access.

C. Using a VPN concentrator which supports dual factor via hardware tokens.

D. Implementing 802.lx with EAP-TILS across the infrastructure.

Answer(s): D

---

18. A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief

A. Agile

B. SDL

C. Waterfall

D. Joint application development

Answer(s): A

---

19. Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

A. Require each Company XYZ employee to use an IPSec connection to the required systems

B. Require Company XYZ employees to establish an encrypted VDI session to the required systems

C. Require Company ABC employees to use two-factor authentication on the required systems

D. Require a site-to-site VPN for intercompany communications

Answer(s): B

---

20. Due to compliance regulations, a company requires a yearly penetration test. The Chief Information

A. The risk of unplanned server outages is reduced.

B. Using documentation provided to them, the pen-test organization can quickly determine areas to focus on.

C. The results will show an in-depth view of the network and should help pin-point areas of internal weakness.

D. The results should reflect what attackers may be able to learn about the company.

Answer(s): D
