Comptia Advanced Security Practitioner (CASRP) Beta Exam

1. In which of the following activities an organization identifies and prioritizes technical, organizational, procedural, administrative, and physical security weaknesses?

A. Social engineering

B. Vulnerability assessment

C. White box testing

D. Penetration testing

Answer(s): B

---

2. John is a security administrator for a large retail company. He wishes to address new threats, what is the most important step for him to take in addressing new threats?

A. Performing a proper risk assessment

B. Performing a vulnerability assessment

C. Ensuring the firewall is properly configured

D. Creating security policies for the new threat

Answer(s): A

---

3. Which of the following statements are true about a smartphone? Each correct answer represents a complete solution. Choose two.

A. It allows the user to install and run more advanced applications based on a specific platform.

B. It can be simple software-based Softphones or purpose-built hardware devices that appear much like an ordinary telephone or a cordless phone.

C. It allows telephone calls to be made over an IP network.

D. It is a mobile phone with advanced PC like capabilities.

Answer(s): A,D

---

4. New technologies can pose unique and new risks that must be managed. Which of the following new technologies poses the most risk due to regulatory compliance?

A. Tablets

B. Smart phones

C. Cloud computing

D. Virtualization

Answer(s): C

---

5. Mark wants to compress spreadsheets and PNG image files by using lossless data compression so that he can successfully recover original data whenever required. Which of the following compression techniques will Mark use?

A. Vector quantization

B. Deflation

C. Adaptive dictionary algorithm

D. Color reduction

Answer(s): B,C

---

6. Which of the following devices allows telephone calls to be made over an IP network such as the Internet instead of the ordinary PSTN system?

A. IP phone

B. Laptop

C. IP camera

D. Smartphone

Answer(s): A

---

7. Which of the following is a log that contains records of login/logout activity or other security-related events specified by the systems audit policy?

A. Process tracking

B. Logon event

C. Object Manager

D. Security Log

Answer(s): D

---

8. Which of the following are the key security activities for the initiation phase? Each correct answer represents a complete solution. Choose two.

A. Determination of privacy requirements.

B. Perform functional and security testing.

C. Initial delineation of business requirements in terms of confidentiality, integrity, and availability.

D. Analyze security requirements.

Answer(s): A,C

---

9. Which of the following is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed by use of a cryptographic hash?

A. Hashing

B. Non-repudiation

C. Code signing

D. Entropy

Answer(s): C

---

10. Which of the following is a security incident in which sensitive or confidential data is copied, transmitted, viewed, or stolen by unauthorized person?

A. Security token

B. Data masking

C. Data breach

D. Data erasure

Answer(s): C

---

11. Collaboration platform offers a set of software components and services that enable users to communicate, share information, and work together for achieving common business goals. What are the core elements of a collaboration platform?

A. Product and service integration

B. Real-time communication

C. Change management

D. Team collaboration

E. Messaging

Answer(s): B,D,E

---

12. Which of the following are the benefits of the Single sign-on? Each correct answer represents a complete solution. Choose three.

A. Reducing password fatigue from different user name and password combinations

B. Increasing IT costs due to lower number of IT help desk calls about passwords

C. Centralized reporting for compliance adherence

D. Security on all levels of entry/exit/access to systems without the inconvenience of re- prompting users

Answer(s): A,C,D

---

13. Which of the following is a document used to solicit proposals from prospective sellers which require a significant amount of negotiation?

A. RFQ

B. RFI

C. RFP

D. RPQ

Answer(s): C

---

14. You are responsible for evaluating, recommending, and directing changes to the Corporate Security Manager in order to ensure the security of assets, facilities, and employees of the organization. What is your designation?

A. Facility manager

B. HR manager

C. Physical security manager

D. Network administrator

Answer(s): C

---

15. Which of the following statements best describe the advantages of Simple Object Access Protocol (SOAP): Each correct answer represents a complete solution. Choose three.

A. It is versatile enough to allow for the use of different transport protocols.

B. It is simple and extensible.

C. It allows easier communication through proxies and firewalls than previous remote execution technology.

D. It is language and platform dependent.

Answer(s): A,B,C

---

16. Which of the following statements are true about OCSP and CRL?

A. The OCSP checks certificate status in real time

B. The CRL is a list of subscribers paired with digital certificate status.

C. The main limitation of CRL is the fact that updates must be frequently downloaded to keep the list current.

D. The CRL allows the authenticity of a certificate to be immediately verified.

Answer(s): A,B,C

---

17. Which of the following standard organizations promulgates worldwide proprietary industrial and commercial standards?

A. IEEE

B. ANSI

C. ISO

D. W3C

Answer(s): C

---

18. You have considered the security of the mobile devices on your corporate network from viruses and malware. Now, you need to plan for remotely enforcing policies for device management and security, which of the following things are includes in the configuration management of mobile devices?

A. Controlling the apps deployed on devices

B. Managing the OS version of devices

C. Supporting other preferred corporate policy

D. Managing application and security patches

Answer(s): B,D

---

19. You work as a security administrator for uCertify Inc. You are conducting a security awareness campaign for the employees of the organization. What information will you provide to the employees about the security awareness program?

A. It improves awareness of the need to protect system resources.

B. It improves the possibility for career advancement of the IT staff.

C. It enhances the skills and knowledge so that the computer users can perform their jobs more securely.

D. It constructs in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Answer(s): A,C,D

---

20. Which of the following statements are true about Mean Time to Repair (MTTR)? Each correct answer represents a complete solution. Choose three.

A. It is the total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time.

B. It is the average time taken to repair a Configuration Item or IT Service after a failure.

C. It represents the average time required to repair a failed component or device.

D. It includes lead time for parts not readily available or other Administrative or Logistic Downtime (ALDT).

Answer(s): A,B,C
