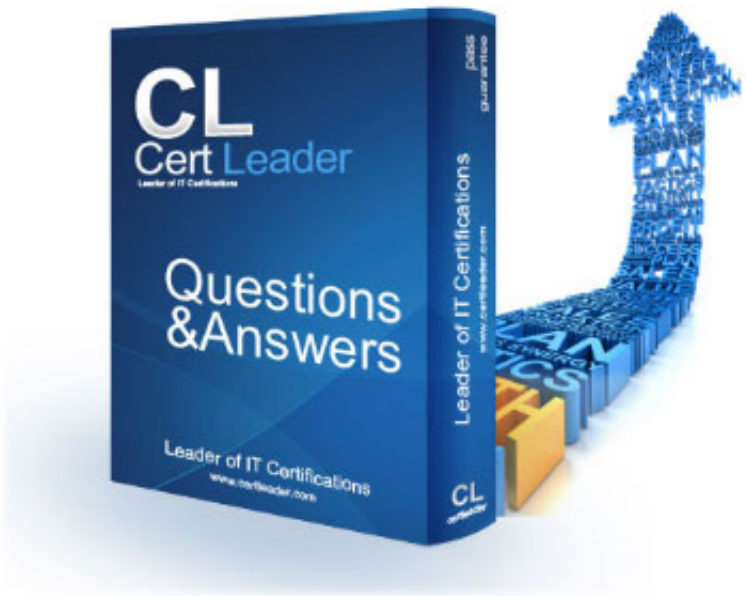
CISSP - Certified Information Systems Security Professional (CISSP)

http://www.certleader.com/CISSP-dumps.html



1.What component of a web application that stores the session state in a cookie can be bypassed by an attacker?

A. An initialization check

B. An identification check

C. An authentication check

D. An authorization check

Answer: C

2. The PRIMARY purpose of a security awareness program is to

A. ensure that everyone understands the organization's policies and procedures.

B. communicate that access to information will be granted on a need-to-know basis.

C. warn all users that access to all systems will be monitored on a daily basis.

D. comply with regulations related to data and information protection.

Answer: A

3. Which of the following is the best practice for testing a Business Continuity Plan (BCP)?

A. Test.before the IT Audit

B. Test when environment changes

C. Test after installation of security patches

D. Test after implementation of system patches

Answer: B

4. Which of the following violates identity and access management best practices?

A. User accounts

B. System accounts

C. Generic accounts

D. Privileged accounts

Answer: C

5. Why must all users be positively identified.prior.to using multi-user computers?

A. To provide access to system privileges

B. To provide access to the operating system

C. To ensure that unauthorized persons cannot access the computers

D. To ensure that management knows what users are currently logged on

Answer: C

6. The three PRIMARY requirements for a penetration test are

A. A defined goal, limited time period, and approval of management

B. A general objective, unlimited time, and approval of the network administrator

C. An objective statement, disclosed methodology, and fixed cost

D. A stated objective, liability waiver, and disclosed methodology

Answer: A

7. A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?

A. The organization's current security policies concerning privacy issues

B. Privacy-related regulations enforced by governing bodies applicable to the organization

C. Privacy best practices published by recognized security standards organizations

D. Organizational procedures designed to protect privacy information

Answer: B

8. An organization is designing a large enterprise-wide document repository system. They plan to have several different classification level areas with increasing levels of controls. The BEST way to ensure document confidentiality in the repository is to

A. encrypt the contents of the repository and document any exceptions to that requirement.

B. utilize Intrusion Detection System (IDS) set drop connections if too many requests for documents are detected.

C. keep individuals with access to high security areas from saving those documents into lower security areas.

D. require individuals with access to the system to sign Non-Disclosure Agreements (NDA).

Answer: C

9. Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

A. poor governance over security processes and procedures

B. immature security controls and procedures

C. variances against regulatory requirements

D. unanticipated increases in security incidents and threats

Answer: A

10. Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?

A. Set up a BIOS and operating system password

B. Encrypt the virtual drive where confidential files can be stored

C. Implement a mandatory policy in which sensitive data cannot be stored on laptops, but only on the corporate network

D. Encrypt the entire disk and delete contents after a set number of failed access attempts

Answer: D

11. During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification. Which of the following is the MOST likely reason for this?

A. The procurement officer lacks technical knowledge.

B. The security requirements have changed during the procurement process.

C. There were no security professionals in the vendor's bidding team.

D. The description of the security requirements was insufficient.

Answer: D

12. Which of the following has the GREATEST impact on an organization's security posture?

A. International and country-specific compliance requirements

B. Security.violations by employees and contractors

C. Resource constraints due to increasing costs of supporting security

D. Audit findings related to employee access and permissions process

Answer: A

13. Which of the following can BEST prevent security flaws occurring in outsourced software development?

A. Contractual requirements for code quality

B. Licensing, code ownership and intellectual property rights

C. Certification.of the quality and accuracy of the work done

D. Delivery dates, change management control and budgetary control

Answer: C

14. During an investigation of database theft from an organization's web site, it was determined that the Structured Query Language (SQL) injection technique was used despite input validation with client-side scripting. Which of the following provides the GREATEST protection against the same attack occurring again?

A. Encrypt communications between the servers

B. Encrypt the web server traffic

C. Implement server-side filtering

D. Filter outgoing traffic at the perimeter firewall

Answer: C

15. Which of the following statements is TRUE regarding value boundary analysis as a functional software testing technique?

A. It is useful for testing communications protocols and graphical user interfaces.

B. It is characterized by the stateless behavior of a process implemented in a function.

C. Test inputs are obtained from the derived threshold of the given functional specifications.

D. An entire partition can be covered by considering only one representative value from that partition.

Answer: C

16. What does an organization FIRST review to assure compliance with privacy requirements?

A. Best practices

B. Business objectives

C. Legal and regulatory mandates

D. Employee's compliance to policies and standards

Answer: C

17. An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

A. Availability

B. Confidentiality

C. Integrity

D. Ownership

Answer: C

18. The 802.1x standard provides a framework for what?

A. Network authentication for only wireless networks

B. Network authentication for wired and wireless networks

C. Wireless encryption using the Advanced Encryption Standard (AES)

D. Wireless network encryption using Secure Sockets Layer (SSL)

Answer: B

19. What is a common challenge when implementing Security Assertion Markup Language

(SAML) for identity integration between on-premise environment and an external identity provider service?

A. Some users are not provisioned into the service.

B. SAML tokens are provided by the on-premise identity provider.

C. Single users cannot be revoked from the service.

D. SAML tokens contain user information.

Answer: A

20. Which of the following are required components for implementing software configuration management systems?

A. Audit control and signoff

B. User training and acceptance

C. Rollback and recovery processes

D. Regression testing and evaluation

Answer: C

21. Why is a system's criticality classification important in large organizations?

A. It provides for proper prioritization and scheduling of security and maintenance tasks.

B. It reduces critical system support workload and reduces the time required to apply patches.

C. It allows for clear systems status communications to executive management.

D. It provides for easier determination of ownership, reducing confusion as to the status of the asset.

Answer: A

22. Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam approaches?

A. Simple Mail Transfer Protocol (SMTP) blacklist

B. Reverse Domain Name System (DNS) lookup

C. Hashing algorithm

D. Header analysis

Answer: D

23. An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

A. Limits and scope of the testing.

B. Physical location of server room and wiring closet.

C. Logical location of filters and concentrators.

D. Employee directory and organizational chart.

Answer: A

24. What should happen when an emergency change to.a system.must be performed?

A. The change must be given priority at the next meeting of the change control board.

B. Testing and approvals must be performed quickly.

C. The change must be performed immediately and then submitted to the change board.

D. The change is performed and a notation is made in the system log.

Answer: B

25. Which of the following is the BEST way to verify the integrity of a software patch?

A. Cryptographic checksums

B. Version numbering

C. Automatic updates

D. Vendor assurance

Answer: A

26. Which one of these risk factors would be the LEAST important consideration in choosing a building site for a new computer facility?

A. Vulnerability to crime

B. Adjacent buildings and businesses

C. Proximity to an airline flight path

D. Vulnerability to natural disasters

Answer: C

27. Which of the following controls is the FIRST step in protecting privacy in an information system?

A. Data Redaction

B. Data Minimization

C. Data Encryption

D. Data Storage

Answer: B

28. Refer.to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.

Which of the following is considered the MOST important priority for the information security officer?

A. Formal acceptance of the security strategy

B. Disciplinary actions taken against unethical behavior

C. Development of an awareness program for new employees

D. Audit of all organization system configurations for faults

Answer: A

29. Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

A. Standards, policies, and procedures

B. Tactical, strategic, and financial

C. Management, operational, and technical

D. Documentation, observation, and manual

Answer: C

30. How does an organization verify that.an.information system's.current hardware and software match the standard system configuration?

A. By reviewing the configuration after the system goes into production

B. By running vulnerability scanning tools on all devices in the environment

C. By comparing the actual configuration of the system against the baseline

D. By verifying all the approved security patches are implemented

Answer: C

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISSP Exam with Our Prep Materials Via below:

http://www.certleader.com/CISSP-dumps.html