ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

Version:Demo

1. How can a forensic specialist exclude from examination a large percentage of operating system files residing on a copy of the target system?

A. Take another backup of the media in question then delete all irrelevant operating system files.

B. Create a comparison database of cryptographic hashes of the files from a system with the same operating system and patch level.

C. Generate a message digest (MD) or secure hash on the drive image to detect tampering of the media being examined.

D. Discard harmless files for the operating system, and known installed programs.

Answer: B

2. Which of the following explains why record destruction requirements are included in a data retention policy?

A. To comply with legal and business requirements

B. To save cost for storage and backup

C. To meet destruction.guidelines

D. To validate data ownership

Answer: A

3. Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

A. Policy documentation review

B. Authentication validation

C. Periodic log reviews

D. Interface testing

Answer: C

4. Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?

A. Access based on rules

B. Access based on user's role

C. Access determined by the system

D. Access based on data sensitivity

Answer: B

5. During an audit of system management, auditors find that the system administrator has not been trained. What actions need to be taken at once to ensure the integrity of systems?

A. A review of hiring policies and methods of verification of new employees

B. A review of all departmental procedures

C. A review of all training procedures to be undertaken

D. A review of all systems by an experienced administrator

Answer: D

6. Disaster Recovery Plan (DRP) training material should be

A. consistent so that all audiences receive the same training.

B. stored in a fire proof safe to ensure availability when needed.

C. only delivered in paper format.

D. presented in a professional looking manner.

Answer: A

7. Are companies legally required to report all data breaches?

A. No, different jurisdictions have different rules.

B. No, not if the data is encrypted.

C. No, companies' codes of ethics don't require it.

D. No, only if the breach had a material impact.

Answer: A

8. Data leakage of sensitive information is MOST often.concealed.by which of the following?

A. Secure Sockets Layer (SSL).

B. Secure Hash Algorithm (SHA)

C. Wired Equivalent Privacy (WEP)

D. Secure Post Office Protocol (POP)

Answer: A

9. A large university needs to enable student.access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?

A. Provide students with Internet Protocol Security (IPSec) Virtual Private Network (VPN) client software.

B. Use Secure Sockets Layer (SSL) VPN technology.

C. Use Secure Shell (SSH) with public/private keys.

D. Require students to purchase home router capable of VPN.

Answer: B

10. Which of the following is a recommended alternative to an integrated email encryption system?

A. Sign emails containing sensitive data

B. Send sensitive data in separate emails

C. Encrypt sensitive data separately in attachments

D. Store sensitive information to be sent in encrypted drives

Answer: C

11. Logical access control programs are MOST effective when they are

A. approved by external auditors.

B. combined with security token technology.

C. maintained by computer security officers.

D. made part of the operating system.

Answer: D

12. Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

A. Concept, Development, Production, Utilization, Support, Retirement

B. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation

C. Acquisition, Measurement, Configuration Management, Production, Operation, Support

D. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal

Answer: B

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

During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.

If the intrusion causes the system processes to hang, which of the following has been affected?

A. System integrity

B. System availability

C. System confidentiality

D. System auditability

Answer: B

14. Which of the following is the MOST beneficial to review when performing an IT audit?

A. Audit policy

B. Security log

C. Security policies

D. Configuration settings

Answer: C

15. Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

A. Network Address Translation (NAT)

B. Application Proxy

C. Routing Information Protocol (RIP) Version 2

D. Address Masking

Answer: A

16. When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

A. Temporal Key Integrity Protocol (TKIP)

B. Wi-Fi Protected Access (WPA) Pre-Shared Key (PSK)

C. Wi-Fi Protected Access 2 (WPA2) Enterprise

D. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

Answer: C

17. Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?

A. It uses a Subscriber Identity Module (SIM) for authentication.

B. It uses encrypting techniques for all communications.

C. The radio spectrum is divided with multiple frequency carriers.

D. The signal is difficult to read as it provides end-to-end encryption.

Answer: A

18. Copyright provides protection for which of the following?

A. Ideas expressed in literary works

B. A particular expression of an idea

C. New and non-obvious inventions

D. Discoveries of natural phenomena

Answer: B

19. Which of the following is a method used to prevent Structured Query Language (SQL)

injection attacks?

A. Data compression

B. Data classification

C. Data warehousing

D. Data validation

Answer: D

20. An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?

A. Data leakage

B. Unfiltered channel

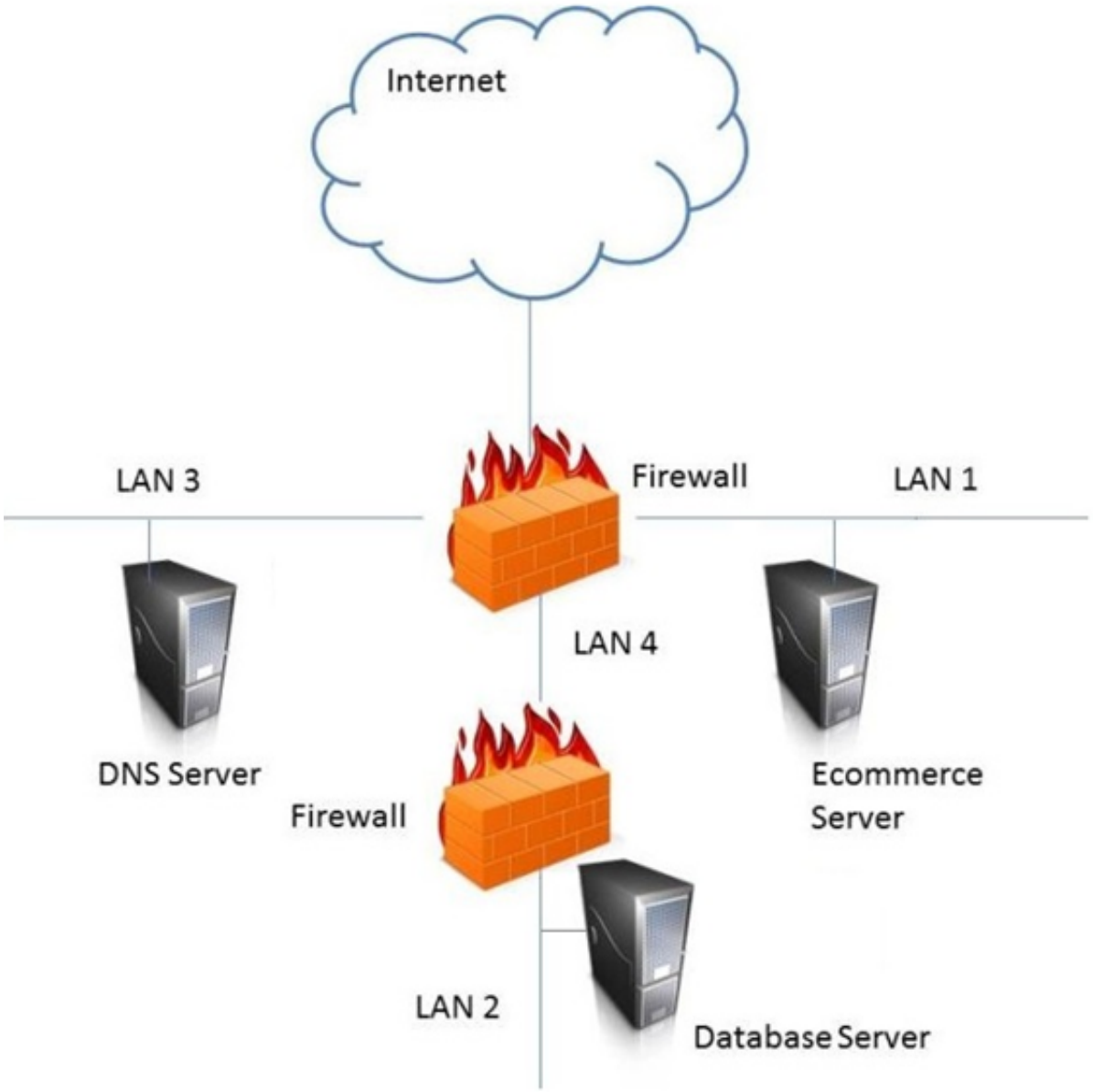
C. Data emanation

D. Covert channel

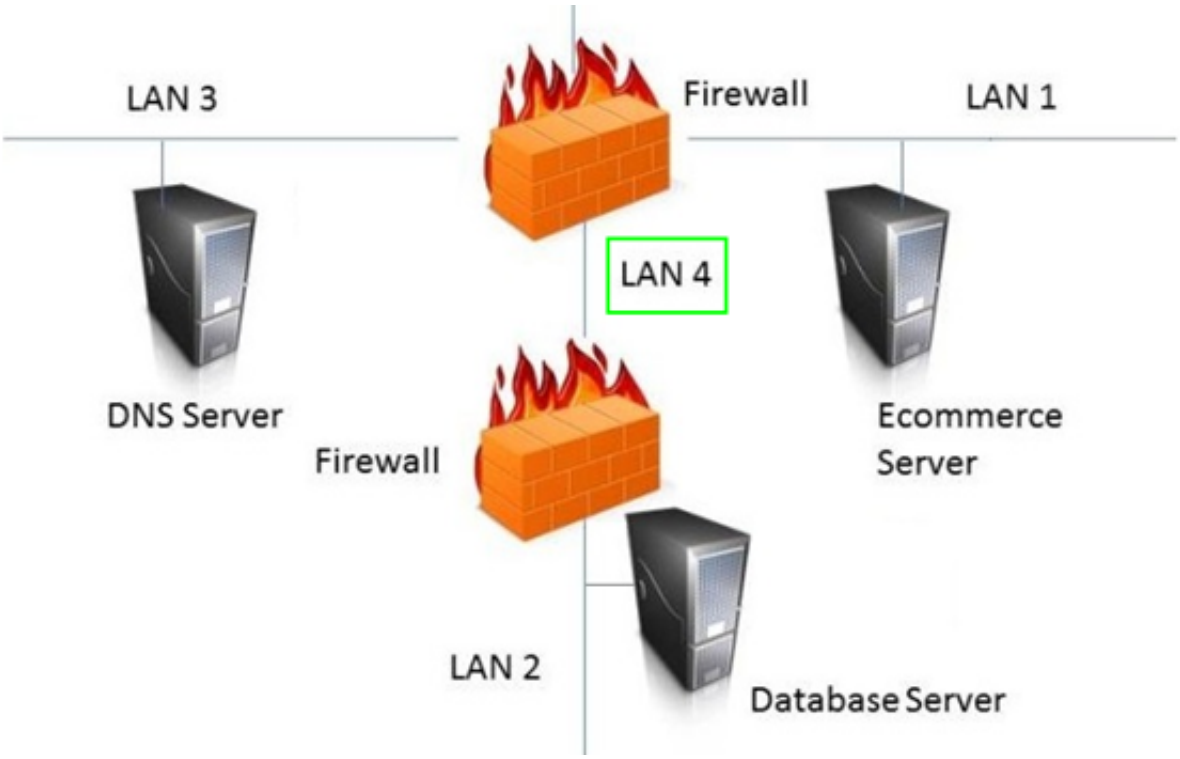
Answer: D

21. HOTSPOT

In the network design below, where.is.the.MOST secure.Local Area Network (LAN).segment to deploy a.Wireless.Access.Point (WAP) that provides.contractors.access to the Internet and authorized enterprise services?


Internet
LAN 3
Firewall
LAN 1
LAN 4
DNS Server
Firewall
Ecommerce Server
LAN 2
Database Server

Answer:



22. Which of the following actions should be performed when implementing a change to a database schema in a production system?

A. Test in development, determine dates, notify users, and implement in production

B. Apply change to production, run in parallel, finalize change in production, and develop a back-out strategy

C. Perform user acceptance testing in production, have users sign off, and finalize change

D. Change in development, perform user acceptance testing, develop a back-out strategy, and implement change

Answer: D

23. Which security.approach.will BEST.minimize.Personally Identifiable.Information (PII) loss from a data breach?

A. A strong breach notification process

B. Limited collection of individuals' confidential data

C. End-to-end data encryption for data in transit

D. Continuous monitoring of potential vulnerabilities

Answer: B

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

During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.

If it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?

A. Availability

B. Integrity

C. Accountability

D. Confidentiality

Answer: D

25. What is one way to mitigate the risk of security flaws in.custom.software?

A. Include security language in the Earned Value Management (EVM) contract

B. Include security assurance clauses in the Service Level Agreement (SLA)

C. Purchase only Commercial Off-The-Shelf (COTS) products

D. Purchase only software with no open source Application Programming Interfaces (APIs)

Answer: B

26. When is security personnel involvement in the Systems Development Life Cycle (SDLC) process MOST beneficial?

A. Testing phase

B. Development phase

C. Requirements definition phase

D. Operations and maintenance phase

Answer: C

27. What is the MOST effective countermeasure to a malicious code attack.against a.mobile system?

A. Sandbox

B. Change control

C. Memory management

D. Public-Key Infrastructure (PKI)

Answer: A

28. Which of the following is an appropriate source for test data?

A. Production.data that is secured and maintained only in the production environment.

B. Test data that has no similarities to production.data.

C. Test data that is mirrored and kept up-to-date with production data.

D. Production.data that has been.sanitized before loading into a test environment.

Answer: D

29. In Business Continuity Planning (BCP), what is the importance of documenting business processes?

A. Provides senior management with decision-making tools

B. Establishes and adopts ongoing testing and maintenance strategies

C. Defines who will perform which functions during a disaster or emergency

D. Provides an understanding of the organization's interdependencies

Answer: D

30. The PRIMARY characteristic of a Distributed Denial of Service (DDoS) attack is that it

A. exploits weak authentication to penetrate networks.

B. can be detected with signature analysis.

C. looks like normal network activity.

D. is commonly confused with viruses or worms.

Answer: C

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

* CISSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year