PRACTICE QUESTIONS

INFORMATION SECURITY AUDITORS MODULE – PART II

1) A system has been patched many times and has recently become infected with a dangerous virus. If antivirus software indicates that disinfecting a file may damage it, what is the correct action?

   a. Replace the file with the file saved the day before
   b. Restore an uninfected version of the patched file from backup media
   c. Back up the data and disinfect the file
   d. Disinfect the file and contact the vendor

2) Which of the following centrally controls the database and manages different aspects of the data?

   a. Data dictionary
   b. Data storage
   c. Access control
   d. Database

3) What is the purpose of polyinstantiation?

   a. To restrict lower-level subjects from accessing low-level information
   b. To create different objects that will react in different ways to the same input
   c. To create different objects that will take on inheritance attributes from their class.
   d. To make a copy of an object and modify the attributes of the second copy

4) When a database detects an error, what enables it to start processing at a designated place?

   a. Data dictionary
   b. Metadata
   c. Checkpoint
   d. Data-mining tool

5) Database views provide what type of security control?

   a. Preventive
   b. Detective
   c. Administrative
   d. Corrective

6) Which of the following is used to deter database inference attacks?

   a. Controlling access to the data dictionary
   b. Partitioning, cell suppression, and small query sets
   c. Partitioning, noise and perturbation, and small query sets
   d. Partitioning, cell suppression, and noise and perturbation

7) If one department can view employees' work history and another group cannot view their work history, what is this an example of?

a. Content-dependent access control
b. Context-dependent access control
c. Separation of duties
d. Mandatory access control

8) What is a disadvantage of using content-dependent access control on databases?

a. It increases processing and resource overhead.
b. It can cause deadlock situations.
c. It can access other memory addresses.
d. It can cause concurrency problems.

9) If security was not part of the development of a database, how is it usually handled?

a. Views
b. Cell suppression
c. Trusted front end
d. Trusted back end

10) When should security first be addressed in a project?

a. During integration testing
b. During design specifications
c. During implementation
d. During requirements development

11) What does operations security deal with?

a. Protecting a system from inception to development to operation to removal
b. Safeguarding information assets resident in the computer.
c. Safeguarding how media is stored, accessed, and destroyed.
d. Assigning access rights and permissions, to ensure that individuals have access only to the resources required to carry out their tasks.

12) Why multiple layers in security are useful?

a. Because security is not operated in single layer
b. Because it's much easier to achieve.
c. Because it makes the attackers task difficult.
d. Because its 100% secure.

13) Firewall is used to enforce _____.

a. Company's network security policy
b. Electrical transmission of data among systems
c. Vulnerabilities assessment strategies.

d. Threats assessment strategies.

14) How can dual-homed firewalls be compromised?

a. If call forwarding is enabled, this security measure can be compromised.
b. If a user makes a request to send an e-mail message through her e-mail client Outlook
c. If the network is an Ethernet network
d. If the operating system does not have packet forwarding or routing disabled.

15) What is a protocol?

a. A set of rules that dictates how computers communicate over networks.
b. A set of rules that dictates how computers exchange a service over networks
c. Is a de facto standard for transmitting data across the Internet.
d. Is the major component of the ping utility.

16) What does the presentation layer, layer 6 deal with?

a. The syntax of the data, not the meaning.
b. The different technologies within different types of networks
c. The dialog (session) between two applications
d. The framing of data.

17) Routers work at which layer?

a. Presentation layer
b. Application layer
c. Network layer
d. Transport layer

18) Which layer provides routing, addressing, and fragmentation of packets?

a. Presentation layer
b. Network layer
c. Application layer
d. Transport layer

19) Which layer prepares data for the network medium by framing it?

a. Layer 1
b. Layer 3
c. Layer 4
d. Layer 2

20) On which layer different LAN and WAN technologies operate?

a. Data link layer
b. Network layer
c. Transport layer
d. Presentation layer

21) A physical security mechanism consisting of a small area with two doors used to hold an individual until his identity can be verified is called a _____.

a. Mantrap
b. Turnstile
c. Holding area
d. Man-in-the-middle

22) How does water suppress a fire?

a. Modifies the chemical combustion elements
b. Reduces the temperature
c. Modifies the chemical combustion elements
d. Reduces the fuel

23) Which of the following fire suppressing agents should not be used in an operations center containing employees?

a. Soda acid
b. Gas
c. Water
d. CO_2

24) Which type of lock uses programmable keypads to restrict access?

a. Preset
b. Device
c. Cipher
d. Complex

25) Which of the following does not describe proper use of a fire extinguisher?

a. Must be inspected yearly
b. Must contain fire suppression agent appropriate for a particular area
c. Must be visible
d. Must be in an area with electrical equipment

26) What is the name of water sprinkler system that keeps pipes empty and doesn't release water until a certain temperature is met and a delay mechanism instituted?

a. Wet
b. Delayed
c. Preaction
d. Dry

27) Which of the following is currently the most recommended water system for a computer room?

a. Wet pipe
b. Dry pipe

c. Deluge
d. Preaction

28) What is plenum space?

a. The screened subnet area within DMZ
b. Open space above dropped ceilings and below raised floors.
c. The unprotected area around the security perimeter fence
d. A VPN tunnel

29) Sometimes basic fencing does not provide the level of protection a company requires. Which of the following combine the functions of intrusion detection systems and fencing?

a. Perimeter
b. PIDAS
c. Closed-circuit TV
d. Acoustic-seismic detection system

30) Piggybacking can be best prevented by which physical controls?

a. Mantrap
b. Fail-safe door
c. Badge readers
d. Turnstile

31) What is ISMS?

a. Information Security Management System
b. Information System Managing Security
c. Integrity System Mitigating Service
d. Integrating Security Management System

32) What is PDCA model?

a. Plan, Do, Collect, Arrange
b. Procure, Develop, Contain, Allow
c. Plan, Do, Check, Act
d. Procure, Develop, Configure, Analyze

33) In this Information age, what is the most import asset of any organization?

a. Machinery
b. Employees
c. Finance Data
d. Data

34) Why is a security policy important to an organization?

a. Provides employees with assistance in their respective jobs.
b. Provides protection from liability due to an employee's actions and control access to trade secrets.
c. Provides management with access to all resources.

d. Provides recognition in market.

35) What is an objective of security policy?

a. To reduce vulnerabilities to a tolerable level and to minimize the effects of threats.
b. To make company staff efficient in their work.
c. To control flow of raw materials to proper destination.
d. To make employees feel they are the sole users of the system.

36) Any compromise in a security policy could lead to _____.

a. Company's loss of sensitive information.
b. Loss of company's overall security architecture.
c. Decrease in company's turnover.
d. Hamper the company's work flow.

37) In this information age, which is the most vulnerable asset of an organization?

a. Machinery
b. Finance
c. Data
d. Employees

38) What could be a lifesaver during a disaster or catastrophe in a company?

a. Network Analyst
b. Security Analyst
c. Tech savvy employee in top management
d. A well written policy

39) How do we better understand policy?

a. A statement of the goals to be achieved by procedures.
b. A statement of the goals to be achieved by guidelines.
c. A statement of the goals to be achieved by standards.
d. A statement of the goals to be achieved by baselines.

40) A security policy does not contain

a. The statement of words which concerns security.
b. The security goal to be achieved.
c. The implementation process of the security.
d. The awareness of security for employees.

NOTE : THIS IS A SAMPLE TEST. THE ACTUAL TEST WILL CONTAIN 90 QUESTIONS.

Answers :

1	(b)	21	(a)
2	(a)	22	(b)
3	(d)	23	(d)
4	(c)	24	(c)
5	(a)	25	(a)
6	(d)	26	(c)
7	(a)	27	(d)
8	(a)	28	(b)
9	(c)	29	(b)
10	(d)	30	(a)
11	(b)	31	(a)
12	(c)	32	(c)
13	(a)	33	(d)
14	(d)	34	(b)
15	(a)	35	(a)
16	(a)	36	(a)
17	(c)	37	(c)
18	(b)	38	(d)
19	(d)	39	(a)
20	(a)	40	(c)