A **Reg. No. :** | | | | | | | | | | |

Question Paper Code: 96C04

B.E./B.Tech. DEGREE EXAMINATION, APRIL 2024

Sixth Semester

Computer Science and Business Systems

19UCB604 - INFORMATION SECURITY

(Regulations 2019)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 1 = 10 Marks)

1. What is "theft of service"? CO1- U

   (a) Unauthorized modification of data. (b) Unauthorized reading of data.

   (c) Unauthorized use of resources. (d)Unauthorized destruction of data.

2. Which component of the CIA triad ensures that information is accessible to authorized users when they need it? CO1 -U

   (a) confidentiality (b) Integrity (c) Availability (d) All the above

3. Which access control model uses a set of rules to determine whether to grant or deny access to a resource? CO1-U

   (a) Mandatory Access Control (b) Role-Based Access Control

   (c) Discretionary Access Control (d) All of the above

4. Which access control model is based on the idea of assigning roles to users and granting access based on their roles? CO1-U

   (a) Mandatory Access Control (b) Role-Based Access Control

   (c) Discretionary Access Control (d) All of the above

5. Which of the following is a critical component of a secure system design? CO1-U

   (a) Regular vulnerability assessments (b) Strong passwords

   (c) Frequent system updates (d) All of the above

6. What is the purpose of system evaluation? CO1-U

(a) To identify system failures and bugs.

(b) To ensure the system meets user requirements and expectations

(c) To improve the efficiency and performance of the system.

(d) To increase the security of the system.

7. Which of the following is not a characteristic of a logic-based system? CO1-U

(a) Formal rules for reasoning

(b) Use of inference rules

(c) Uncertainty handling mechanisms

(d) Representation of knowledge in a declarative manner

8. What is the purpose of two-factor authentication (2FA)? CO1-U

(a) To allow users to use multiple devices to access a system

(b) To prevent unauthorized access to a system by requiring two different forms of authentication

(c) To encrypt data transmissions between a user and a system

(d) To provide an additional layer of protection against malware

9. What is the most common security threat to an operating system? CO1-U

(a) Malware (b) Hardware failure (c) Human error (d) Natural disaster

10. Which of the following is an example of a security policy that can be enforced by an operating system? CO1-U

(a) Password complexity requirements (b) Antivirus software installation

(c)Regular system backups (d)Network traffic monitoring

PART – B (5 x 2= 10 Marks)

11. If the lock picker is trustworthy, the assumption is valid. Define the case? CO1-U

12. The customer information stored in the company's database. Apply access control mechanism would you recommend using for this scenario. CO1-U

13. Define the term Vulnerability analysis. CO3-Ana

14. List any two IDS. Mention its category of classification CO1-U

15. Why Database Security is important? CO1-U

PART – C (5 x 16= 80Marks)

16.	(a)	Consider a scenario where a hacker gains unauthorized access to a company's database of customer information relating to CIA triad procedure.	CO2- App	(16)
		Or		
	(b)	Apply the protection methodology when a person X runs an organization by mean time facing a constant danger discuss in detail about protection	CO2- App	(16)
17.	(a)	How confidentiality polices is been practiced and make a detailed note on it?	CO1-U	(16)
		Or		
	(b)	Discuss any two Policies with its benefits and key components.	CO1-U	(16)
18.	(a)	A healthcare organization has recently implemented a new electronic health record system. Apply the security of this system in terms of protecting patient data.	CO2- App	(16)
		Or		
	(b)	A new employee named John joined the agency. John is a manager, but he has a history of unauthorized access to sensitive information in his previous job. The agency has decided to implement a stricter access control policy for John. Can the agency implement a stricter access control policy for John using the model?	CO2-App	(16)
19.	(a)	A company uses a cloud-based storage system to store sensitive customer data, including credit card information. One day, an employee receives an email that appears to be from the company's IT department, requesting that they enter their login credentials to verify their account. The employee enters their credentials without realizing that the email was a phishing attempt. Apply type of malicious behavior occurred in this scenario, and what could be the potential consequences of this action?	CO2- App	(16)
		Or		

	(b)	You are a security analyst for a large organization. The organization's IT department recently upgraded the operating system on all of the organization's computers, and you have been tasked with ensuring the security of the new operating system. One of the organization's employees reports that their computer has been infected with malware. You discover that the malware was able to exploit a vulnerability in the operating system. Apply steps would you take to prevent similar incidents from occurring in the future and improve the security of the organization's operating systems?	CO2-App	(16)
20.	(a)	How would you explain operating system security in terms of information security?	CO1-U	(16)
		Or		
	(b)	Develop a comprehensive database security plan for a large organization, including risk assessment, threat modeling, and implementation of security controls such as access control, encryption, auditing and monitoring, backup and recovery, and vulnerability management.	CO1-U	(16)