Reg.No. : | | | | | | | | | | | | |

Question Paper Code: U6C02

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

Sixth Semester

Computer Science and Business Systems

21UCB602 INFORMATION SECURITY

(Regulations 2021)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1.	List the principles of a software design.	CO1-U
2.	If the lock picker is trustworthy, the assumption is valid. Define the case.	CO2- App
3.	Define Spatio -Temporal model.	CO1-U
4.	The customer information stored in the company's database. Apply access control mechanism would you recommend using for this scenario.	CO2- App
5.	Define confinement problem	CO1-U
6.	Apply how can access control mechanisms help address the confinement problem?	CO2- App
7.	Define the term user security?	CO1-U
8.	List down the capabilities of intrusion detection?	CO1-U
9.	Mention the best practices of enterprise security?	CO1-U
10.	Write down the five steps of Enterprise information security architecture?	CO1-U

PART – B (5 x 16= 80 Marks)

11.	(a)	Evaluate the strengths and weaknesses of different access control models (e.g., discretionary access control, mandatory access control) in enforcing security policies.	CO2- App	(16)
		Or		
	(b)	Propose a comprehensive incident response plan for a medium-sized organization that addresses detection, containment, eradication, and recovery from security incidents.	CO2- App	(16)

12.	(a)	How do access control models contribute to regulatory compliance, such as GDPR or HIPAA?	CO2- App	(16)
		Or		
	(b)	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)
13.	(a)	Compare and contrast the effectiveness of virtualization and sandboxing in addressing the confinement problem.	CO1-U	(16)
		Or		
	(b)	How can the company evaluate the website to identify any potential issues? What are the benefits and limitations of different evaluation methods in this context?	CO1-U	(16)
14.	(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, 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)

15. (a) What steps would you take to address the security vulnerability in the critical application and mitigate the potential risks to the institution? CO1-U (16)

Or

(b) What are the key components of a database security architecture and how do they work together to protect a database system? (database security) CO1-U (16)