

Reg. No.																			
----------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code	12495
---------------------	-------

B.E. / B.Tech - DEGREE EXAMINATIONS, NOV / DEC 2023

Third Semester

Computer Science and Engineering (Cyber Security)

20SCPC302 - CYBER SECURITY ESSENTIALS

(Regulations 2020)

Duration: 3 Hours

Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

- | | <i>Marks,
K-Level, CO</i> |
|--|-------------------------------|
| 1. What is the role of encryption in computer security. | <i>2,K2,CO1</i> |
| 2. Mention the importance of access control in protecting sensitive data. | <i>2,K1,CO1</i> |
| 3. Identify the purpose of access control lists in an operating system's security model. | <i>2,K2,CO2</i> |
| 4. Justify how rootkits can manipulate system calls to avoid detection. | <i>2,K3,CO2</i> |
| 5. Define "malware" and provide an examples of a malware types. | <i>2,K2,CO3</i> |
| 6. Difference between authentication and authorization. | <i>2,K4,CO3</i> |
| 7. Point out the consequence of organizational security with compliance standards. | <i>2,K1,CO4</i> |
| 8. Differentiate cyber attack and traditional form of attacks. | <i>2,K3,CO4</i> |
| 9. Summarize the value of having an incident response plan as part of cyber security management. | <i>2,K2,CO5</i> |
| 10. List out the impact of IoT on data privacy. | <i>2,K1,CO5</i> |

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11. a) Explain the authentication and access control in cyber security in detail. *13,K2,CO1*
- OR**
- b) Discuss in detail about the different attacks in world wide web. *13,K2,CO1*
12. a) Justify the assess use of formal methods in ensuring the security of operating systems and discuss how formal verification techniques contribute to the design and implementation of secure operating systems. *13,K3,CO2*
- OR**
- b) Explain in detail about the principles and considerations involved in designing secure networking protocols and discuss how the security of protocols is used in different networks. *13,K2,CO2*

13. a) Examine the reliability authentication methods for personal computer security. Discuss the strengths and weaknesses of authentication and propose strategies for securing devices from virus and other intruders. *13,K4,CO3*
- OR**
- b) Analyze the concept of authorization systems by giving the strong credentials for using physical and logical security to safeguarding system against a wide range of potential threats. *13,K4,CO3*
14. a) Explain the principles and practices of integrating application security into the development lifecycle for identifying and monitoring threads in every stage. *13,K2,CO4*
- OR**
- b) Discuss the responsibilities of organizations in handling data breaches ethically and transparently for preventing attacks. *13,K2,CO4*
15. a) Examine the significance of incident response planning in security and discuss the key components of an incident response plan and the importance of regular testing. *13,K4,CO5*
- OR**
- b) Discover the emerging trends in cyber warfare and analyze the applicability of international law to cyber warfare. *13,K4,CO5*

PART - C (1 × 15 = 15 Marks)

16. a) Examine the potential threats and vulnerabilities introduced by the advent of computer security and discuss the implications for current cryptographic methods for preparing cyber security defenses against threats. *15,K4,CO1*
- OR**
- b) Analyze the relationship between data privacy and the principle of confidentiality and discuss how organizations can uphold data privacy while maintaining the confidentiality of sensitive information. *15,K4,CO4*