Sub Code: SCS-301 **ROLL NO……..……..**

III SEMESTER EXAMINATION, 2023 – 24

II[nd] year , B Tech – Computer Science & Engineering

Cyber Security and Investigation Techniques

Duration: 3:00 hrs **Max Marks: 100**

Note: - Attempt all questions. All Questions carry equal marks. In case of any ambiguity or missing data, the same may be assumed and state the assumption made in the answer.

Q 1.	Answer any four parts of the following. a) Differentiate between various cyber threats, including cyber warfare, cyber-crime, cyber terrorism, and cyber espionage. Provide examples of each and discuss their implications. b) Discuss the importance of a comprehensive cybersecurity policy. Outline key components that should be included in such a policy to address diverse cyber threats. c)Explain the concept of a nodal authority in the context of cybersecurity. Discuss the role it plays in coordinating and implementing cybersecurity measures. d)Discuss the role of education in addressing cybersecurity challenges. Explore how raising awareness and promoting cybersecurity education can contribute to a safer digital environment. e) Explore the intersection of cybersecurity and privacy. Discuss how cybersecurity measures can be balanced to protect sensitive information while respecting individual privacy rights. f) Provide an overview of the field of cybersecurity. Discuss its significance in the modern digital landscape and highlight the primary objectives of cybersecurity.	5x4=20
Q 2.	Answer any four parts of the following. a) Explore different authentication methods used in cyber security. Compare and contrast methods such as passwords, biometrics, and cryptographic tokens. b) Discuss the role of cryptography in cyber security. Explain how cryptographic techniques contribute to safeguarding sensitive information. c) Define ethical hacking and discuss its significance in cyber security. Explain how ethical hacking differs from malicious hacking and its role in identifying vulnerabilities. d) Discuss the role of Intrusion Detection Systems (IDS) in cyber security. Explain how IDS detects and responds to potential security threats. e) Discuss the importance of security policies in cyber security. Explain how organizations can implement effective security policies to protect against cyber threats. f) Provide an overview of cyber security safeguards. Discuss the role these safeguards play in protecting digital systems and networks.	5x4=20
Q 3.	Answer any two parts of the following. a) Provide an overview of securing HTTP applications and services. Discuss basic security measures for HTTP, including encryption and authentication. Explain the importance of securing communication over the web and common challenges associated with HTTP security. b) Explore the fundamentals of securing SOAP (Simple Object Access Protocol)	10x2= 20

	services. Discuss authentication, encryption, and other security measures applicable to SOAP-based web services. Compare the security considerations for SOAP with those for HTTP applications. c) Discuss the role of identity management in web services. Explore how identity is established and managed in the context of web applications. Explain the importance of secure identity management for maintaining the integrity and confidentiality of user information.	
Q 4.	Answer any two parts of the following. a) Discuss various types of intrusions, such as physical theft, abuse of privileges, unauthorized access, and malware infections. Explore the impact of each on information security. b) Explain the role of anti-malware software in preventing and detecting malware. Discuss Network-Based Intrusion Detection Systems (NIDS) and Network-Based Intrusion Prevention Systems (NIPS). c) Discuss the significance of Host-Based Intrusion Prevention Systems (HIPS) in securing individual computer systems. Explore its role in preventing unauthorized activities on hosts.	10x2= 20
Q 5.	Answer any two parts of the following. a) Explore the concept of system integrity validation. Discuss the methods and significance of validating system integrity in ensuring security. b) Explain the purpose of Security Information Management (SIM) systems. Discuss how SIM systems collect and analyze security data to manage incidents and enhance security. c) Discuss the importance of network session analysis in preventing security threats. Explain how it helps identify and address potential issues.	10x2= 20

****