[This question paper contains 4 printed pages.]

Your Roll No……

Sr. No. of Question Paper : 15070

Unique Paper Code : 2932813601

Name of the Paper : Cyber Security

Name of the Course : **B.Tech (CSE)**

Semester : VI

Duration: 3 Hours Maximum Marks: 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. Attempt **five** questions in all, including question no. 1, which is compulsory.
3. A non-programmable scientific calculator is allowed.
4. **All** questions carry equal marks.

1. (a) A hospital stores patient records digitally. One day, records are modified without authorization, and later, the system becomes unavailable for doctors during emergencies. Analyze which components of the CIA triad are affected and recommend cybersecurity controls for each.

(b) Employees unknowingly connect to a fake wireless hotspot named similarly to the company's Wi-Fi. Identify the attack type and explain how wireless security policies can prevent such incidents.

(c) A financial institution depends on RSA encryption for secure transactions, but is concerned about future quantum attacks. Explain how quantum computing threatens modern cryptography.

(d) Explain why having a structured incident response plan is essential for minimizing damage and restoring operations quickly.

(e) Explain why continuous monitoring and secure configuration practices are important in maintaining system security.

(f) Discuss why endpoint security is equally important in a cybersecurity strategy.

(3 × 6 = 18)

2. (a) Multiple employees in an organization use the same password for personal social media and office systems. Attackers exploit leaked credentials. Analyze vulnerabilities in the scenario. Suggest cybersecurity practices, authentication methods, and organizational policies to reduce credential compromise.

(b) A bank wants to redesign its online banking platform to improve security against fraud and identity theft. Design a cybersecurity plan using encryption, hashing, digital signatures, and access-control policies. Explain how each mechanism contributes to confidentiality, integrity, and authentication.

(9 × 2 = 18)

3. (a) System administrators use Telnet for remote access to servers instead of SSH. Explain why Telnet is insecure. Compare Telnet, SSH, and HTTPS with respect to confidentiality, authentication, and integrity. Suggest migration steps to secure protocols.

(b) Employees report that their devices automatically connect to a Wi-Fi network named similarly to the company's official Wi-Fi. Sensitive credentials are leaked. Identify the attack type. Explain how such attacks work. Suggest technical and policy-based measures to prevent recurrence.

(9 × 2 = 18)

4. (a) A junior employee in an organization exploits a misconfigured sudo policy on a Linux system, gaining administrator access to confidential HR files. Identify the security weakness involved. Explain the concept of privilege escalation and discuss how least privilege, access control mechanisms, auditing, and secure Linux configuration can prevent such attacks.

(b) A banking application written in C crashes when a user enters very long input values. Later, attackers exploit this flaw to execute malicious code. Explain buffer overflow vulnerability and how attackers exploit it. Recommend secure coding techniques, compiler protections, memory safety controls, and testing approaches.

(9 × 2 = 18)

5. (a) A company migrates customer data to cloud storage, but due to improper access configuration, confidential files become publicly accessible online. Identify the cloud security weakness involved. Explain risks associated with cloud misconfiguration, insecure APIs, and shared responsibility models. Suggest security controls for prevention.

(b) A hacker gains access to smart locks, cameras, and thermostats in a connected smart home ecosystem by exploiting default passwords and unencrypted communication. Analyze the vulnerabilities and suggest security mechanisms for device authentication, encryption, firmware updates, and network isolation.

(9 × 2 = 18)

6 (a) A smart city uses IoT sensors whose data is stored in cloud platforms for analytics and decision-making. Analyze combined security challenges in IoT and Cloud Computing, including data privacy, authentication, scalability, and attack surfaces. Suggest a secure architecture.

(b) A cloud-hosted Linux web server has open unnecessary ports, weak SSH passwords, outdated packages, and unrestricted root login. Explain how to harden this Linux system. Discuss secure SSH configuration, access controls, service minimization, monitoring, and patching strategies. (9 × 2 = 18)

(200)