B.E. INFORMATION TECHNOLOGY 4TH YEAR-1ST SEMESTER EXAMINATION– 2025

Subject: Network Security (Hons.)

Time: 3 hrs. **Full Marks: 100**

(Note: Answer must be brief and to the point, and answers of all parts of a question should be written together)

CO1 (20)	Q.1 ***Answer any five:*** a. Explain vulnerabilities due to neighbor discovery (ICMP) protocol attack. What is Steganography? b. How MAC layer packet transmissions occur in a secure way? Define threats and attacks. c. Describe attacking techniques of the following: Sniffing, Spoofing, Storms and Buffer overflow with proper example of each. d. Differentiate between network security, information security and cyber security based on their common parameters (e.g., data, viruses, scope, protect, attack, threat, security etc.). e. Define three aspects of security. Distinguish active and passive attacks with proper examples. f. Explain DDoS, masquerade, brute force and replay attacks with proper use cases. 4x5
CO2 (20)	Q.2 ***Answer any two:*** a. Define PGP Certificate and its utility? Explain different phases of SSL session establishment. State design philosophy of Transport Layer Security (TLS). 3+4+3 b. Give a framework of confidentiality and authentication mechanism for one-to-many email transmission. Explain the SSL architecture. Describe how the Replay Attack (Earlier SSL handshake messages are replayed) is countered by a particular feature of SSL. 2+4+4 c. Explain: Security system in transport layer (including connection state, session state, record protocol with format, handshake, change cipher spec, alert protocols, and master secret creation). Differentiate between SSL and TLS as securities in transport layer. 7+3
CO3 (25)	Q.3 ***Answer (a) and any one from (b) and (c):*** a. What are the security services provided by IPSec? Discuss different parameters in Security Association Databases and Security Policy Databases. Write short notes on i) IKE protocol and ii) Encapsulation Security Protocol. 2+(3+2)+3x2 b. Differentiate between i) stateless and state-ful firewalls, and ii) IDS and IPS in firewalls. How do IDS and IPS work in firewalls? Write functionalities of different types of IDS in firewalls. 3x2+3+3 c. What are the capabilities and limitations of firewalls? Explain working principles of SOCKS as circuit level gateway. Explain application-level filtering technique in a gateway. 2x2+4+4
CO4 (20)	Q.4 ***Answer any one:*** a. Define various access control techniques and access control systems (at least four from each)? Describe phase-wise handshaking protocol in Secure Socket Layer (SSL) authentication. "Non-repudiation is essential than repudiation"- explain with proper justification? Write short notes on i) Kerberos authentication and ii) MD5 for authentication. 4x2+4+2+3x2 b. Write short notes on: i) Remote authentication and ii) Password authentication. Distinguish between EAPOL and TKIP (protocols). With the principle of "least privileged" is it possible to have too much authorization and what happens when there is too much authorization? Demonstrate AES Counter & Cipher-Block Chaining modes relative to 802.11i. 4x2+4+2+3x2
CO5 (15)	Q.5 ***Answer any one:*** a. Explain various types of Phishing attacks with their respective use cases. Define Sybil attack and how to prevent it. What are the symptoms and preventive measurements of such attacks? 6+3+3+3 b. Explain Intrusion detection in real life scenarios. Explain use cases of different types of Wormhole attacks. Write different techniques/algorithms/models to counter such type of attacks. 3+6+6

-: Course Outcomes :-

CO1: Identify and explain different terms & terminologies related to network security.

CO2: Illustrate different application layer encryption techniques and transport layer security protocols and algorithms.

CO3: Sketch the network layer protocols and related algorithms in detail and study uses, types, deployment and limitations of a firewall.

CO4: Demonstrate the knowledge of different types of access control, authorization and authentication mechanisms in wired and wireless networks.

CO5: Comprehend the basic technologies for security of web services.