B.E. INFORMATION TECHNOLOGY 4TH YEAR-1ST SEMESTER EXAMINATION– 2024

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. What are the importance of trusted systems? Differentiate passive attack from active attack with example. b. Explain weaknesses of TCP/IP/UDP suite. List out different social engineering attacking techniques. c. Explain vulnerabilities due to neighbor discovery (ICMP) protocol attack. What is Steganography? d. How MAC layer packet transmissions occur in a secure way? Define threats and attacks. e. Differentiate between Network Security and Cyber Security on the following parameters: data, viruses, strikes against, and security. f. Describe three attacking techniques from the followings: Sniffing, Spoofing, Storms and Distributed DoS. g. Differentiate among: i) Masquerade and Brute-force Attacks and ii) Security Attacks, Security Mechanisms and Security Services. 4x5
CO2 (20)	Q.2 ***Answer (a) and any one from (b) and (c):*** a. Illustrate the working principle of PGP. Explain DNS lookup process with DNSSEC. Give a framework of confidentiality or authentication mechanism for one-to-many email transmission. 5+3+2 b. Discuss the salient features of SSL. Explain in detail the payment capture transaction supported by SSL/TLS. Describe how any one of the following is countered by a particular feature of SSL. i) Replay Attack: Earlier SSL handshake messages are replayed. ii) Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client. 2+4+4 a. 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. Compare between transport and tunnel mode in IP security. Write a short note on Encapsulating Security Payload (ESP). Explain: Security system in IP layer (including modes with respective pkt. formats, security association with database, security policy databases, inbound, and outbound pkt. processing). 3+4+6 b. Explain Transport Mode in IPSec communication. How application gateway works? State default automated key management protocols for IPsec (i.e., Oakley and ISAKMP). 6+2+(2+2) c. Define firewall. Differentiate between IDS and IPS. Explain firewall deployment with DMZ. What are the limitations of firewall? 2+3+5+2
CO4 (20)	Q.4 ***Answer any one:*** a. What do you mean by access control and access control matrix? What are the benefits of authorization? Define different types of access control techniques with their associated technologies. What is Public-Key Authentication? Demonstrate different Public-Key Authentication methods. (2+2)+2+5+3+6 b. Explain different types of authorization systems. With the principle of "least privileged" is it possible to have too much authorization? What happens when there is too much authorization? Why do we need non-repudiation? Demonstrate AES Counter & Cipher-Block Chaining modes relative to 802.11i. (5+3)+2+2+(4+4)

CO5 (15)	Q.5 ***Answer any two:***
	a. Explain various types of Phishing attacks with their respective use cases. What are the symptoms and preventive measurements of such attacks? 8+3+4
	b. Define Wormhole attacks. Explain various use cases of various type of Wormhole attacks. Write different techniques/algorithms/models to counter such type of attacks. 3+6+6
	c. Define Sybil attack and how to prevent it. What is intrusion detection (ID)? Explain Intrusion detection in real life scenarios. How do you distinguish host based IDs and network based IDs? (2+2)+2+3+(3+3)

-: Course Outcomes :-

CO1: Identify and explain different terms & terminologies related to network security. (K2)

CO2: Illustrate different application layer encryption techniques and transport layer security protocols and algorithms. (K3)

CO3: Sketch the network layer protocols and related algorithms in detail and study uses, types, deployment and limitations of a firewall. (K3)

CO4: Demonstrate the knowledge of different types of access control, authorization and authentication mechanisms in wired and wireless networks. (K3)

CO5: Comprehend the basic technologies for security of web services. (K2)