Name:

Enrolment No:

UPES

End Semester Examination, May 2025

Course: IT Network Security | **Semester : VI**

Program: B. Tech (CSE), Cyber Security & Forensics | **Time : 03 hrs.**

Course Code: CSSF3024 | **Max. Marks: 100**

Instructions: Please attempt according to the provided time and given weightage.

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	In the context of firewall, explain tiny fragment attack and mention a countermeasure for this attack.	**2+2**	**CO3**
Q 2	Discuss privilege escalation attacks in cybersecurity and list their types (names only).	**3+1**	**CO2**
Q 3	Describe the four types of Internet Access Policies. *(Provide a brief explanation for each.)*	**4**	**CO6**
Q 4	During Firewall penetration testing, how is a **Firewalk** performed?	**4**	**CO3**
Q 5	With respect to VPN functionality, what is encapsulation? List at least two most common VPN encapsulation protocols.	**2+2**	**CO5**

SECTION B
(4Qx10M= 40 Marks)

Q 6	(i) Define RAID technology. (ii) In RAID, how do mirroring and striping differ in terms of data storage and performance?	**5+5**	**CO6**
Q 7	(i) Explain the principle of Direct Sequence Spread Spectrum (DSSS) in wireless communication. (ii) For the binary data 101, compute the transmitted encoded sequence using the Pseudo-Random Noise (PN) code 110101. Show each step of the encoding process and the final transmitted bitstream. **Hint:** Use XOR as the encoding operation.	**3+7**	**CO5**
Q 8	(i) Describe the term system hardening. *(in about 25--30 words.)* (ii) Match the items in Column A with their appropriate corresponding items in Column B. *(Write only the correct pairings.)*	**3+7**	**CO1, CO2, CO3, CO4, CO5**

Column A	Column B
MIMO-OFDM	Software/hardware bug or configuration weakness that is unknown to the vendor
Unstructured threats	Overloading a target system with excessive requests
ICMP Scanning	Air interface for 4G and 5G broadband wireless communication
Replay Attacks	Redirecting traffic to malicious sites
Zero-Day Vulnerability	Exploitation of captured data without modification.
DNS Poisoning	Unskilled individuals who attack the network out of curiosity
DoS Attack	Identifying live hosts and devices

Q 9	(i) Define the following security terms: Confidentiality, Integrity, Availability, Authentication, and Non-repudiation. *(Provide a concise definition for each.)* **OR** (ii) (a) Write the standard **tabular structure** of a packet filtering firewall rule and provide a concrete example. (b) Write the structure of an IDS **alert rule** (e.g., using Snort syntax) with a specific example. Describe how these rules operate in their respective systems, addressing: (1) information inspected and (2) action taken when a match occurs.	**10** **10**	**CO3**
	SECTION-C **(2Qx20M=40 Marks)**		
Q 10	(i) Using labeled diagrams, explain the working principles of **RAID 0**, and **RAID 1**. For each type, clearly indicate: (a) How data is organized across disks (b) Its key advantage and (c) Its limitation. **OR** (ii) Using labeled diagrams, explain the working principles of **RAID 3**, **RAID 5**. For each type, clearly indicate: (a) How data is organized across disks (b) Its key advantage and (c) Its limitation.	**20** **20**	**CO6**
Q 11	(i) Discuss a generic digital signature method that combines asymmetric encryption and hashing. *(Use diagram to explain the process, considering a scenario where integrity is a priority but confidentiality is not.)* (ii) How does a Pure Honeypot differ from a High-Interaction Honeypot? *(Mention at least four key differences.)*	**10+10**	**CO2, CO3**