Name: **Enrolment No:**	UPES UNIVERSITY OF TOMORROW

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Term Examination, May 2024

Course: IT Security Management **Semester: IV**
Program: MBA DB **Time : 03 hrs.**
Course Code: DSIT8011 **Max. Marks: 100**

Instructions:

SET 1
SECTION A
10Qx2M=20Marks

S. No.		Marks	CO
Q 1	Attempt all questions.		
I.	What is the primary goal of encryption? a) To prevent unauthorized access to data b) To increase the speed of data transmission c) To compress data for storage efficiency d) To hide the existence of data	**2**	**CO1**
II.	Which encryption technique involves applying a mathematical function to data to produce a fixed-size string of characters, ensuring data integrity? a) Symmetric encryption b) Asymmetric encryption c) Hashing d) Steganography	**2**	**CO1**
III.	Which of the following is NOT a common type of malware? a) Spyware b) Ransomware c) Worm d) Pop-up blocker	**2**	**CO1**
IV.	What is the primary function of a firewall in a network security system? a) To physically block unauthorized access to a network b) To monitor and control incoming and outgoing network traffic c) To encrypt all data transmitted over a network d) To detect and remove malware from a network	**2**	**CO1**
V.	What is the primary objective of cybersecurity? a) To eliminate all cyber threats completely b) To reduce the risk of unauthorized access, data breaches, and cyber attacks	**2**	**CO1**

	c) To guarantee 100% safety of data at all times d) To ensure that all software is bug-free		
VI.	Which of the following is NOT considered a common cybersecurity threat? a) Malware b) Phishing c) Hardware failure d) Social engineering	**2**	**CO1**
VII.	What is the purpose of an IT security policy? a) To restrict employee access to the internet b) To ensure compliance with legal and regulatory requirements c) To promote transparency in company operations d) To limit the use of encryption technologies	**2**	**CO1**
VIII.	Which of the following is a proactive measure against cyber threats? a) Intrusion detection systems b) Regular data backups c) Reactive patch management d) Allowing unrestricted access to company networks	**2**	**CO1**
IX.	What is the term used to describe a malicious program that replicates itself and spreads to other computers or devices? a) Firewall b) Trojan horse c) Virus d) Encryption	**2**	**CO1**
X.	Which of the following is an example of a social engineering attack? a) DDoS attack b) Brute force attack c) Phishing attack d) SQL injection attack	**2**	**CO1**
SECTION B **4Qx5M= 20 Marks**			
	Attempt **all** questions.		
Q2	What is the purpose of encryption?	**5**	**CO2**
Q3	Why is IT security required?	**5**	**CO2**
Q4	What are Threats , Vulnerabilities and Risks?	**5**	**CO2**
Q5	What is a firewall?	**5**	**CO2**
SECTION-C **3Qx10M=30 Marks**			
	Attempt any **three** questions		
Q6	You are an IT administrator at a small company. One of your employees reports receiving an email from what appears to be the company's IT	**10**	**CO3**

	department, asking them to click on a link to update their login credentials due to a security breach. What should you advise the employee to do? What are the potential threats possible if the employee clicks and provide login credentials?		
Q7	During a routine security audit, you notice unusual network traffic originating from an employee's workstation late at night when the employee is not supposed to be working. What could be causing the unusual behaviour over the network?	**10**	**CO3**
Q8	What are various malware a company should be aware and implement measures for?	**10**	**CO3**
Q9	What is Bell-LaPadula Model? How it helps organization to implement IT security?	**10**	**CO3**
SECTION-D **30 Marks**			
Q10	Attempt all the question XYZ Corporation, a multinational company specializing in financial services, recently fell victim to a sophisticated malware attack that compromised sensitive customer data and caused significant disruptions to its operations. The attack, which originated from a phishing email, exploited vulnerabilities in the company's network security infrastructure, bypassing existing defenses and spreading rapidly across its systems. In response to this incident, XYZ Corporation decided to strengthen its cybersecurity posture by implementing a comprehensive firewall solution. Questions: **Each question carry 5 marks** 1. Describe what malware is and how it poses a threat to organizations like XYZ Corporation. 2. Explain the potential consequences of a malware attack on a company's operations, reputation, and financial stability. 3. Discuss the role of a firewall in preventing malware attacks and safeguarding organizational networks. 4. Outline the various types of firewalls available and their respective features and capabilities in combating malware threats. 5. Detail the steps XYZ Corporation should take to deploy and configure a firewall effectively to protect against future malware attacks. 6. Explore the importance of employee education and training in recognizing and mitigating the risks associated with malware infections.	**30**	**CO3**