RV COLLEGE OF ENGINEERING®

(An Autonomous Institution affiliated to VTU, Belagavi)

III Semester Master of Technology (Common to MCE / MCN)

CYBER SECURITY

Time: 03 Hours ***Maximum Marks: 100***

Instructions to candidates:

1. Answer FIVE full questions selecting one from each unit (1 to 5).
2. Each unit consisting of two questions of 20 marks each.

		UNIT-1	**M**	**BT**	**CO**
1	a	Describe the working principle of symmetric encryption and how it maintains data confidentiality. Discuss its benefits and limitations, providing examples of widely used symmetric encryption algorithms and their applications.	10	2	1
	b	Illustrate with a neat diagram concept of *DNS* and the associated attacks.	10	2	1
		OR			
2	a	Define the concept of virtualization and its role in modern computing. Discuss its benefits and challenges in cybersecurity, explain how it enhances system security.	10	2	1
	b	Define a firewall and explain its role in network security. Discuss different types of firewalls and their functionalities with example.	10	1	2
		UNIT-2			
3	a	A multinational financial institution experienced a series of phasing attacks that tricked employees into downloading a malicious attachment. Once opened, the malware installed itself as a part of a botnet using a Fast-Flux network, making it difficult for security teams to track the origin of the attack. Justify how these attributes are used by attackers? Also explain how to mitigate these types of attacks.	10	3	2
	b	Illustrate with an example concepts of Phishing, Smishing, Vishing, and Mobile Malicious Code.	10	1	1
		OR			
4	a	A newly popular mobile antivirus app on Android claimed to offer "free security updates" but secretly installed malware. Instead of protecting the user, the app engaged in click fraud by generating fake ad clicks in the background while also stealing login credentials from mobile banking apps. Justify how these attributes are user by attackers? Also explain how to mitigate these types of attacks.	10	3	3
	b	What are tunneling techniques? Explain how attackers use VPNs, SSH tunnels, and DNS tunneling for evading network security controls.	10	2	2
		UNIT-3			
5	a	SELECT text, user, timestamp FROM blog_entries where user =' x'; SELECT uname, pwd from users; -- '; What are the implications of above command? Explain its consequences and way to mitigate these kind of attacks.	10	3	3
	b	Illustrate the integer overflow vulnerability? Explain with a case study how it used by the attackers.	10	1	1
		OR			

6	a	Explain the following in detail with an example. i) Race Conditions ii) Cross-Site Scripting (XSS)	10	4	3
	b	You are a security analyst for a large e-commerce platform that recently experienced a data breach. During investigation, it was discovered that attackers gained unauthorized access to customer data stored in the database. Further analysis revealed that the breach was due to a SQL Injection vulnerability in the checkout page of the website. Explain how SQL Injection works, the potential impact on the organization, and recommend preventive measures to mitigate such risks in the future.	10	3	4

UNIT-4

7	a	Illustrate the major differences between worms and viruses.	10	2	1
	b	Explain the following Evading Detection and Elevating Privileges in detail with an example i) Virtual Machine Obfuscation ii) Persistent Software Techniques	10	2	2
		OR			
8	a	Define spyware and explain its various types. How do attackers use spyware to steal sensitive user information, and what counter measures can be implemented to mitigate such attacks?	10	3	3
	b	Describe the process of a Man-in-the-Middle (MitM) attack. What are the different types of MitM attacks, and how can organizations protect against them?	10	3	4

UNIT-5

9	a	Illustrate any three major benefits of memory forensics to handle malware incidents.	10	1	1
	b	Why hash codes or values are important to demonstrate the integrity of digital evidence?	10	3	2
		OR			
10	a	A hospital's patient database is encrypted by ransomware, preventing doctors from accessing critical medical records. The attackers demand a Bitcoin ransom. The hospital contacts digital forensic experts to investigate and recover data. Outline the key steps taken by forensic investigators in the ransomware attack. Why is immediate containment critical in such incidents?	10	4	3
	b	Discuss the legal and ethical considerations that must be followed during the collection and analysis of digital evidence.	05	3	2
	c	Differentiate between live systems forensics and dead system forensics. In what situations would an investigator prefer to analyze a live system instead of a dead one?	05	2	2