U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

May 2023 Semester End Make-Up Examinations

Programme: B.E. **Semester: VII**
Branch: Information Science and Engineering **Duration: 3 hrs.**
Course Code: 20IS7PCISF **Max Marks: 100**
Course: Information Security and Digital Forensics **Date: 17.05.2023**

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

UNIT - I

1	a)	Illustrate how packet filtering firewall decides whether to drop or forward the packet to next network connection.	**08**
	b)	How is static filtering different from dynamic filtering of packets? Describe.	**06**
	c)	Explain the working of Dual-Homed host firewalls with a neat diagram.	**06**

OR

2	a)	How firewalls are categorized based on the generation? Explain the features of each generation firewall.	**08**
	b)	How computer security can be improved in Small Office/ Home Office (SOHO) setting? Describe.	**06**
	c)	Describe the utility used to protect organisation's systems from misuse.	**06**

UNIT - II

3	a)	What are the issues associated with implementing wireless IDPS? Describe.	**06**
	b)	Explain the features of the tool that collects copies of packets from network and analyses them.	**06**
	c)	Describe three basic criteria upon which effectiveness of biometric technologies are evaluated.	**08**

OR

4	a)	What is the role of Network-based IDPS in monitoring network traffic and identifying attacks? Explain.	**08**
	b)	Describe the features of an IDPS that tracks the network connection between internal and external systems using a state table.	**06**
	c)	How active vulnerability scanners are different from passive vulnerability scanners? Explain the features of both.	**06**

UNIT - III

5	a)	List the legal issues involved with creating and using logs.	**08**
	b)	Justify the statement "Audit logs are important in investigations".	**04**
	c)	Which are the sources of an evidence for an investigator? Explain.	**04**
	d)	What is an intrusion detection? List various types of intrusions.	**04**

UNIT - IV

6	a)	What is DNS poisoning? Why it is used? Describe the steps involved in one DNS poisoning technique.	**08**
	b)	How ***tcpdump*** performs statistical analysis on the network packets extracted? Describe.	**06**
	c)	Describe the features of the following tools: (i) EtherDetect Packet Sniffer (ii) Omnipeek.	**06**

UNIT - V

7	a)	How an SQL injection attack is done? What are the steps used to investigate the same? Describe.	**06**
	b)	When does buffer overflow occur? What are the effects of buffer overflow and how it can be detected?	**06**
	c)	Describe the nature and consequences of the following attacks: (i) cryptographic Interception (ii) URL interpretation attack	**08**

****