U.S.N.										

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

Autonomous Institute Affiliated to VTU

February / March 2023 Semester End Main 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: 24.02.2023**

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)	What are the most common threats to the network security system, and how will they be mitigated?	**05**
	b)	How will user authentication and authorization be managed for accessing sensitive data and resources?	**05**
	c)	Your organization is looking to upgrade its firewall solution. Based on this scenario, compare and contrast two different firewall architectures - Screened Host Firewalls and Dual-Homed Host Firewalls recommend the best solution for the organization.	**10**

OR

2	a)	An organization wants to improve the security of their remote access systems by using biometric access controls. What factors should they consider when choosing a biometric system, and how can they ensure that the system is effective in preventing unauthorized access?	**05**
	b)	what biometric access controls are, and how they differ from traditional authentication methods such as passwords and security tokens?	**05**
	c)	A network administrator has noticed an increase in network scans from unknown IP addresses. What tools and techniques can be used to investigate the source of these scans and determine whether they are a threat to the network?	**10**

UNIT - II

3	a)	A financial organization is concerned about the potential harm that could be caused by malicious insiders. They are interested in implementing a padded cell system to prevent any harm caused by insiders. How would you explain the concept of a padded cell system to the organization and its potential benefits?	**05**
	b)	A large multinational corporation is concerned about advanced persistent threats (APTs) targeting their network. How could the implementation of a honeypot help mitigate this risk?	**05**

c) An airport is looking to improve the speed and efficiency of its security check-in process. The airport is considering implementing biometric access control for boarding gates and baggage areas. What are the potential benefits and challenges of using biometric technology in an airport setting, and how would you go about designing a biometric access control system to meet the airport's needs? **10**

OR

4 a) You are the IT manager of a large research facility, and you are responsible for securing sensitive data and equipment that are used by the scientists and engineers. You have decided to implement a biometric access control system to enhance the security of the facility and to prevent unauthorized access. **05**

How would you design and implement the biometric access control system, and what challenges and considerations would you need to take into account?

b) You are the security manager of a large e-commerce company, and you are responsible for protecting the company's online assets and data from cyber attacks and security threats. You have decided to implement an intrusion detection and prevention system (IDPS) to enhance the security of the company's network and systems. **05**

How would you design and implement the IDPS, and what benefits and challenges would you expect to encounter?

c) You are the Chief Security Officer of a large financial institution, and you are concerned about the increasing number of cyber attacks that target your network and systems. You want to improve your organization's security posture by using honeypots, honeynets, padded cell systems, **10**

UNIT - III

5 a) An organization is concerned about the security of their IIS logs and wants to ensure that they are maintained in a credible state. What steps should the organization take to ensure that their IIS logs are credible and can be used as evidence in an investigation? **05**

b) A company has suffered a network security breach and needs to perform a forensic investigation to determine the cause and extent of the breach. What steps should they take in the investigation process, and what types of log files and network data should they analyze to gather evidence? **05**

c) An organization has suffered a data breach and needs to quickly gather information about the attack. What log files should the organization examine and how can they use this information to identify the source of the intrusion and prevent future attacks? **10**

UNIT - IV

6 a) The analyst has determined that the website is suffering from a Buffer Overflow. What is the purpose of a Buffer Overflow and how does it work? How can the analyst mitigate this type of attack on the website? **05**

b) How would you use DNS poisoning techniques and ARP table analysis to determine the cause of the security breach and gather evidence to support your investigation? **10**

c) The analyst has discovered a compromised system and has gathered several files as evidence. How should the analyst go about verifying the authenticity and integrity of the gathered evidence to ensure that it can be used in court if necessary? **05**

UNIT - V

7 a) You are a web developer working on an online shopping website. Your website allows users to leave product reviews, and these reviews are displayed to other users on the product page. One day, you receive reports from users that a malicious script has been injected into the product reviews, causing pop-up ads to appear on the page and steal their personal information. **05**
How would you identify the cause of the problem?
How would you prevent this type of attack from happening again in the future?

b) The analyst has determined that the website is suffering from Cookie Poisoning. What is the purpose of Cookie Poisoning and how does it work? How can the analyst mitigate this type of attack on the website? **05**

c) How important is the use of secure protocols such as HTTPS in protecting web communications from eavesdropping and tampering **10**

******