Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
MID TERM EXAMINATION - APR 2023

Semester : Semester II & IV - 2022 & 2021
Course Code : CSE2060
Course Name : CSE2060 - Information Security and Management
Program : CBD,CSG,ISD,IST

Date : 17-APR-2023
Time : 2PM - 3:30PM
Max Marks : 50
Weightage : 25%

Instructions:
(i) Read all questions carefully and answer accordingly.
(ii) Question paper consists of 3 parts.
(iii) Scientific and non-programmable calculator are permitted.
(iv) Do not write any information on the question paper other than Roll Number.

PART A

ANSWER ALL THE QUESTIONS **(10 X 1 = 10M)**

1. Aditya wants to improve the security of the small company where he works as a security manager. He comes to the conclusion that the company should do a better job of concealing the type of computer, operating system, software, and network connections it employs. Adithya wishes to implement which security principle?

a) Obscurity (CO2) [Knowledge]
b) Layering
c) Diversity
d) Limiting

2. Your senior colleague, Chintan, has emailed you about a contract with one of the clients. You're asked to accept the offer, which you do. After 2 days. Chintan claims he never sent a message. This scenario violates which of the CIA triads?

a) Authentication (CO1) [Knowledge]
b) Confidentiality
c) Integrity
d) Non-Repudiation

3. Meena is an accountant at MHD Infotech. Without sufficient authority and management approval, she modifies the voucher dates in TALLY. Which major principle is most likely violated by the accountant's actions?

a) Integrity (CO1) [Knowledge]
b) Confidentiality
c) Availability
d) Confidentiality, Availability, and Integrity

4. Which of the following best describes the current state of network security?

a) More knowledge is required for attacks than for security (CO1) [Knowledge]

b) Little knowledge is required for attacks than for security

c) Little functionality is required for attacks than for security

d) More functionality is required for attacks than for security

5. A help desk representative receives a call from someone posing as a technical assistant who wants to update some type of information and requests identifying user details that can later be used to gain access. Which of the following attack types has occurred?

a) Pharming (CO2) [Knowledge]

b) Social engineering

c) Phishing

d) Shoulder surfing

6. Which of the following is an example of a security risk caused by malicious human activity?

a) an employee who misunderstands operating procedures (CO2) [Knowledge]

b) an employee who accidentally deletes customer records

c) an employee who inadvertently installs an old database on top of the current one

d) an employee who intentionally destroys data or other system components

7. Toyota employees can gain remote access to sensitive data. Many salespeople spend a significant amount of time in public and use their downtime to catch up on business. Which of the following matters the most to the organisation?

a) Virus infection (CO2) [Knowledge]

b) Social engineering

c) Dumpster diving

d) Shoulder surfing

8. The attacker, Noof, is attempting to divert traffic in a small office. That office has its own mail server, DNS server, and NTP server because their job is so important. Noof takes over the DNS server and redirects www.google.com to his IP address. Office workers who visit Google are now redirected to the noof's machine. What is the name of this kind of attack?

a) MAC Flooding (CO1) [Knowledge]

b) Smurf Attack

c) DNS spoofing

d) ARP Poisoning

9. The administrative assistant dials a help desk number. She received an email informing her that the corporate bank account would be closed if she did not respond with specific personal information within 48 hours. Which of the following types of attacks has occurred?

a) Pharming (CO2) [Knowledge]

b) Social engineering

c) Phishing

d) Shoulder surfing

10. The Development Life Cycle of Security Systems is defined as a_____

a) series of processes and procedures which enables development teams create software and applications in a manner that significantly increases security risks, eliminate security vulnerabilities and reducing costs. (CO1) [Knowledge]

b) series of processes and procedures which enables development teams create risk and vulnerability blueprints.

c) .series of processes and procedures which enables development teams create software and applications of enterprise implementation.

d) series of processes and procedures which enables development teams create software and applications in a manner that significantly reduces security risks, eliminate security vulnerabilities and reducing costs

PART B

ANSWER ALL THE QUESTIONS **(4 X 5 = 20M)**

11. Sophie works as a contractor for a large government agency. She has access to sensitive information and is in charge of the agency's network. Sophie, on the other hand, is dissatisfied with her boss and decides to launch a malicious attack on the agency's network. She gains network access and steals sensitive data by using a USB drive containing malware. Identify the Asset, Threat, Threat Agent, Vulnerability, Exploit, and Risk in the scenario above. Justify your strategy.

(CO1) [Comprehension]

12. What exactly is an insider threat? What are the different kinds of insider threats? What are the potential consequences of the threat, as well as the threat mitigation programmes?

(CO2) [Comprehension]

13. Describe in detail the deadly sins of software security.

(CO2) [Comprehension]

14. Imagine that you work for a software development company as a security analyst. Your team is getting ready to start a new project to develop an online store for a customer. What steps would you take as part of the SecSDLC to guarantee that the platform is safe and resistant to cyberattacks? Please give a thorough response that outlines all the necessary actions you would take at each stage of the SecSDLC.

(CO1) [Comprehension]

PART C

ANSWER ALL THE QUESTIONS **(2 X 10 = 20M)**

15. You are a security analyst at a large financial services company. One of your key responsibilities is to ensure the security of sensitive customer data, including financial transactions and personal information. Using the McCumber Cube, describe how you would address the following security scenario:

Scenario: A hacker has gained access to a database containing sensitive customer information. The hacker has stolen customer names, addresses, social security numbers, and account information. Using the McCumber Cube, describe how you would address this security scenario by addressing the following questions:

a. What information characteristics are relevant to the above scenario?
b. What information states are relevant to this scenario?
c. What security countermeasures would you implement to mitigate this security threat?

(CO1) [Application]

16. A financial organisation has just learned that a group of hackers have accessed its internet banking system without authorization, giving them the ability to monitor and transfer money from user accounts. Although it is unknown how the hackers got access to the platform, it is assumed that they used a software flaw to their advantage. What procedures did the hacker follow to enter this network? In order to defend against attacks, discuss the role that fundamental security concepts play.

(CO2) [Application]