Roll No.

Total No. of Questions : 09

Total No. of Pages : 02

MCA (Sem–2)
INFORMATION SECURITY AND CYBER LAW

Subject Code : PGCA1932

M.Code : 79619

Date of Examination : 22-05-2024

Time : 3 Hrs.

Max. Marks : 70

INSTRUCTIONS TO CANDIDATES :

1. SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.
2. SECTION - B & C have FOUR questions each.
3. Attempt any FIVE questions from SECTION - B & C carrying TEN marks each.
4. Select atleast TWO questions from SECTION - B & C

SECTION-A

1. Write short notes on :

a What is a firewall in information security?

b What is an intrusion detection system in information security?

c What is penetration testing in information security?

d What is cyber law?

e What is a cyber crime?

f What is cyber stalking?

g What is identity theft?

h What is hacking?

i What is phishing?

j What is malware?

SECTION-B

2 What are some common threats to database security, such as unauthorized access, SQL injection attacks, and data leakage, and how can they be prevented or mitigated? What are some best practices for securing databases, such as access control, encryption, and data masking, and how can they be implemented in different types of database systems?

3 What are some common threats to each aspect of the CIA triad, and how can they be prevented or mitigated? How can organizations balance the need for security with the need for accessibility and usability of their data?

4 What is Role-Based Access Control (RBAC) in information security, and how does it help organizations manage access to their resources based on job functions and responsibilities? How is RBAC different from other access control models, such as Discretionary Access Control (DAC) and Mandatory Access Control (MAC)?

5 What are Denial-Of-Service (DoS) attacks and rootkits in information security, and how do they work to disrupt or compromise the availability, integrity, and confidentiality of data and systems? What are some common types of DoS attacks, such as flooding, amplification, and distributed DoS (DDoS), and how can they be prevented or mitigated?

SECTION-C

6 What is the role of IDS in detecting potential security breaches, and what are the different types of IDS used to monitor network traffic and system activity? What are some best practices for implementing a firewall and IDS in an organization, and how can they be used together to improve overall security posture?

7 What are cryptographic algorithms, and how are they used in information security to protect data confidentiality, integrity, and authenticity? What are the different types of cryptographic algorithms, and what are their strengths and weaknesses?

8 How can security policies be effectively communicated and enforced throughout an organization, and what are some best practices for maintaining and updating security policies over time? What are some examples of cyber laws and regulations, and how do they impact information security practices in different industries and jurisdictions?

9 What are some commonly used internet security protocols and standards, such as SSL/TLS, IPsec, and DNSSEC, and how do they help to secure communication and data exchange over the internet? How do these protocols and standards work to provide confidentiality, integrity, and authenticity of information, and what are some best practices for implementing them in an organization?

NOTE : Disclosure of Identity by writing Mobile No. or Marking of passing request on any paper of Answer Sheet will lead to UMC against the Student