

Course Name : MSCCS

Subject Name : Cyber Security Techniques

Subject Code : MSCCS-103

Date : 18-02-2026

Time : 11:30AM TO 01:45PM

Max Marks : 70

Section A

Q.-1. Answer the following (Attempt any three) (30)

- (1) Define cyber crime. Discuss its categories, challenges, complexities, and effects on individuals, organizations, and national security.
- (2) Explain malware in detail. Discuss different types of malware such as viruses, worms, trojans, spyware, ransomware, and botnets.
- (3) Discuss E-Commerce security issues. Explain threats, vulnerabilities, and security mechanisms used in securing online transactions.
- (4) Explain Cyber Security Risk Management. Discuss risk identification, risk assessment, risk mitigation, and risk treatment strategies.
- (5) Explain computer forensics in detail. Discuss its objectives, phases, tools, and challenges faced during forensic investigations.

Section B

Q.-2. Write short notes on any four of the following topics. (20)

- (1) What is Information Security? State the objectives of Information Security Policy.
- (2) What is Cyber Security Assurance Framework?
- (3) Define social engineering. Discuss its types, techniques, real-world examples, and preventive measures.
- (4) Explain the concept of security assurance. Discuss how assurance helps in improving trust in information systems.
- (5) Discuss vulnerability assessment and penetration testing. Explain their role in cyber security risk reduction.
- (6) Explain common network-based attacks. Discuss techniques used by attackers and corresponding defense mechanisms.

Section C

Q.-3. Choose the correct answer from the options given below (10)

(1) Which is CIA triad component?

- | | |
|-------------------|-----------------|
| A) Availability | B) Authenticity |
| C) Accountability | D) Accuracy |

(2) What is availability?

- | | |
|---------------------|--------------------|
| A) Data backup | B) Data access |
| C) Data correctness | D) Data encryption |

(3) What is malware?

- | | |
|----------------------|-----------------------|
| A) Security software | B) Malicious software |
| C) Hardware fault | D) OS error |

(4) Which is a malware type?

- | | |
|----------|-------------|
| A) Virus | B) Firewall |
| C) IDS | D) Router |

(5) What is cyber crime?

- | | |
|-------------------|-----------------|
| A) Legal activity | B) Online crime |
|-------------------|-----------------|

C) Hardware crime

D) Data backup

(6) What is risk management?

A) Risk ignoring

B) Risk reduction

C) Risk analysis

D) Risk acceptance

(7) What is a certificate authority?

A) Key generator

B) Trust provider

C) Data backup

D) User manager

(8) What is encryption?

A) Data hiding

B) Data encoding

C) Data decoding

D) Data deletion

(9) What is network security?

A) Data security

B) System security

C) Network protection

D) Application security

(10) What is authentication?

A) User identification

B) Data encryption

C) Data backup

D) Data filtering

Section D

Q.-4. State whether the following statements are true or false

(10)

- (1) Policies are more detailed than procedures
- (2) Phishing uses fake emails to steal data
- (3) IDS prevents attacks automatically
- (4) Wireless security protects Wi-Fi networks
- (5) Digital forensics deals with digital evidence
- (6) Cyber security policies are optional for organizations
- (7) Network threats include malware attacks
- (8) VPN provides secure communication tunnel
- (9) PKI manages digital certificates
- (10) Web application security prevents SQL injection
