Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 90251

M.C.A. DEGREE EXAMINATIONS, APRIL/MAY 2022.

Second Semester

MC 4205 – CYBER SECURITY

(Regulations 2021)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is cyber security risk management?

2. How to reduce the impact of cyber threats in your organization?

3. What is the role of education awareness in cyber security?

4. What are the key classification of information?

5. How passwords are stored in your personal computer?

6. Which type of firewall used for the following scenario? A School wants to allow its students to retrieve any information from World Wide Web resources on the Internet. To help provide efficient service, the School want to know what site have been visited and what files from those site have been fetched, particularly popular files will be cached locally?

7. What is meant by bot and botnets?

8. Distinguish between Firewalls and Intrusion detection.

9. What is the impact of cyber security assessment in an organization?

10. Define security audit.

PART B — (5 × 13 = 65 marks)

11. (a) List out the goals of confidentiality policy and explain the Bell-LaPadula Model and its limitations. (13)

Or

(b) (i) Explain the various cyber security policies required for an organization. (8)

(ii) Write the difference between Vulnerability, Threat and Risk. (5)

12. (a) Explain the operating guidelines for implementing mobile device security policies. (13)

Or

(b) What is an incident response plan for cyber security? Explain how to manage a data breach with the 6 phases in the incident response plan. (13)

13. (a) (i) Suppose Adams works in the accounting department during the shift between 8.00 am and 5.00 pm., Monday through Friday. Any legitimate access attempt by Adams should be made during those times through a workstation in the accounting department offices. Explain suitable authentication mechanism for the above situation. (8)

(ii) Write the difference between identification and authentication? (5)

Or

(b) (i) Firewalls are targets for penetrators. Why are there few compromises of firewalls? (7)

(ii) Cite a reason why an organization might want two or more firewalls on a single network. (6)

14. (a) Discuss the best practices to defend against malware. (13)

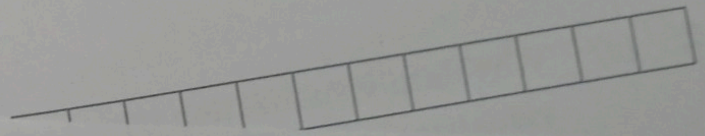
Or

(b) Explain the challenges in Computer Forensics. (13)

15. (a) Discuss the best practices for security compliance in an organization. (13)

Or

(b) Describe how to analyze the security risk in computing system. (13)



PART C — (1 × 15 = 15 marks)

16. (a) Discuss the disaster management and for an airline, what are its most important assets? What are the minimal computing resources it would need to continue business for a limited period (up to two days)? What other system or processes could its use during the period of the disaster?

Or

(b) Discuss the ways to plan a vulnerability test over a web application using OWASP ZAP tool.

———————