Reg. No. : □□□□□□□□□□□□

Question Paper Code : 30147

M.C.A. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 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. List the security governance principles in cyber security.

2. Discuss about security model.

3. State the use of human resources security.

4. Describe mobile device security.

5. Name the four authentication techniques.

6. Compare servers and virtual servers.

7. How can supply chains improve security?

8. Discuss about business continuity planning.

9. List the four main uses of security audit.

10. Describe the steps to improve security monitoring.

PART B — (5 × 13 = 65 marks)

11. (a) Explain in detail about information risk management.

Or

(b) Discuss the Bell-LaPadula Model with suitable diagram.

12. (a) Explain information classification in information security.

Or

(b) Discuss in detail about the different phases in incorporating security into system development life cycle.

13. (a) Explain the business risk of end user developed applications, in detail.

Or

(b) (i) Describe Firewall and its types. (7)

(ii) Describe the IPsec used protocols to secure the IP network traffic. (6)

14. (a) (i) What is Malware Protection? Explain the Common Types of Malwares. (7)

(ii) Define Cryptography and list its features. (6)

Or

(b) Identify the need for vulnerability management? Explain the four stages of vulnerability management.

15. (a) (i) Define risk reporting and explain its types. (6)

(ii) Summarize the key points included in a risk report. (7)

Or

(b) Describe security compliance monitoring and discuss in detail about the steps for creating a cyber-security compliance program.

PART C — (1 × 15 = 15 marks)

16. (a) Evaluate the ten cybersecurity best practices to prevent cyber attacks in 2022.

Or

(b) Point out the top ten critical web application security risks ranked by Open Web Application Security Project (OWASP). Discuss any three categories with example.

————————

12. (a) Explain information classification in information security.

Or

(b) Discuss in detail about the different phases in incorporating security into system development life cycle.

13. (a) Explain the business risk of end user developed applications, in detail.

Or

(b) (i) Describe Firewall and its types. (7)

(ii) Describe the IPsec used protocols to secure the IP network traffic. (6)

14. (a) (i) What is Malware Protection? Explain the Common Types of Malwares. (7)

(ii) Define Cryptography and list its features. (6)

Or

(b) Identify the need for vulnerability management? Explain the four stages of vulnerability management.

15. (a) (i) Define risk reporting and explain its types. (6)

(ii) Summarize the key points included in a risk report. (7)

Or

(b) Describe security compliance monitoring and discuss in detail about the steps for creating a cyber-security compliance program.

PART C — (1 × 15 = 15 marks)

16. (a) Evaluate the ten cybersecurity best practices to prevent cyber attacks in 2022.

Or

(b) Point out the top ten critical web application security risks ranked by Open Web Application Security Project (OWASP). Discuss any three categories with example.

————————