

**EXAMINATION PAPER**

**FACULTY: COMPUTER SCIENCE & MULTIMEDIA**

**COURSE: MASTER OF COMPUTER SCIENCE**

**YEAR/SEMESTER: FIRST / ONE**

**MODULE TITLE & CODE: Cyber Security : CS 123**

**DATE:**

**TIME ALLOWED: 3 HOURS  START: 1:00 PM FINISH: 4:00 PM**

**Instruction to candidates**

1. This question paper has THREE (3) Sections.
2. Answer all **7** questions in Section A, VSAQ
3. Answer **7** questions out of 9 in Section B, SAQ.
4. Answer **2** questions out of 3 in Section C, LAQ.
5. No scripts or answer sheets are to be taken out of the Examination Hall.
6. Lengthy answers do not win more marks. Students are advised to write clear and concise answer with valid relevant examples

***Do not open this question paper until instructed***

*(Candidates are required to give their answers in their own words as far as practicable)*

**SECTION A**

**Very Short Answer Questions**

**Attempt all seven (7) questions [2 × 7 = 14]**

1. What is hacking?
2. Write the importance of Enumeration in Cyber Security.
3. What is the difference between a Virus and a Worm?
4. What is a backdoor application?
5. What are different types of wireless threats?
6. Explain rooting in mobile devices.
7. What is IoT Device Hacking?

**SECTION B**

**Short Answer Questions**

**Attempt only seven (7) questions out of eight (9) questions [7 × 8 = 56]**

1. Footprinting plays an important role in CyberSecurity. Justify with necessary techniques for footprinting. ( UNIT 2: Foot printing and Reconnaissance)  (8)
2. What is TCP communication flags used for? Write the meaning of SYN, ACK, FIN, URG, PSH, RST flags and illustrate them with a diagram for three way handshake. . (UNIT 3: Scanning Networks) (2+4+2)
3. Discuss various Social Engineering countermeasures techniques with suitable examples. (UNIT 9: Social Engineering) (8)
4. What is DoS and DDoS attacks? State some techniques to mitigate DDoS attacks. ( UNIT 10: Denial of Service) (2+6)
5. Write short notes on the following attack vectors:  (UNIT 1: Introduction to Ethical Hacking) (2+2+2+2)
   1. Phishing Attack
   2. Botnet
   3. Insider Attack
   4. Zero-day attack
6. What is an Intrusion Detection System? Discuss with a few examples how IDS detects an intrusion. UNIT 12: Evading IDS, Firewalls and Honeypots) (2+6)
7. What is SQL Injection? Mention its techniques with proper examples. ( UNIT 15: SQL Injection) (2+6)
8. Explain cloud computing with their deployment models. Explain any four threats related to cloud computing. (UNIT 19: Cloud Computing) (3+5)
9. Explain public key and private key in Cryptography. Write the difference between Symmetric and Asymmetric Encryption? (UNIT 20: Cryptography) (3+5)

**Group C**

**Long Analytical or Case Question**

**Attempt any two (2) questions out of three (3) questions [2 × 15 = 30]**

1. Imagine you are appointed as Cyber Security specialist in an organization. The organization has few issues with their web server as it was getting hacked time and again. What steps would you follow in order to prevent the server from further hacking? Explain with your proper audit plan. (UNIT 5: Vulnerability Analysis) (10+5)
2. You are hired as a System Security Officer in a Bank. The bank employees gets lots of phising emails in their inbox. CEO asks you to train all employees in the bank to differentiate the legitimate mail from a Phising email. Write down the things you would like to suggest in the training. ( UNIT 9: Social Engineering) (15)
3. Imagine you work as a System Administrator on a newly established company. What would you suggest your CEO about the organization’s network so that it becomes very much secure. Illustrate your network design that includes cloud computing, proper firewall and disaster recovery with suitable diagram.  (UNIT 19: Cloud Computing) (8+7)