This question paper contains 2 printed pages. Roll No. .....

Master of Computer Applications
MCAE501: Cyber Security
Unique Paper Code: 223402501
Semester V
Nov-Dec 2022
Year of admission: 2020

Time: Three Hours **Max. Marks: 70**

(Write your Roll No on the top immediately upon receipt of this question paper.)

Attempt all questions.

All parts of a question must be answered together.

Question 1. Define **any three** of the below: [3+3+3=9]

a. SCADA Control Systems
b. ARP Spoofing
c. COI in the context of control systems.
d. AIC in the context of Critical Infrastructure Protection.

Question 2. [6+4=10]

a. Give appropriate answers for the case study as per the Indian IT Act 2000:

Alice received a threat over mail (Suppose Gmail) which is sent by Bob. Both are residents of India.

i. Who are the originator, addressee, and intermediary?
ii. Which section(s) of the IT Act 2000 can be applied to the intermediary for such threats over E-mail?
iii. Can the adjudicating officer book the sender of the E-Mail under Section 66A?

b. Differentiate between cognizable and non-cognizable offences.
c. What do you understand by the compounding of offences?

Question 3. Suppose the user passwords are stored in a device in an encrypted form:

[5+5=10]

a. How can you find the passwords in plaintext as an attacker? Explain your answer with the help of an example.
b. What precautions should you take while storing passwords as a defender? Explain Your answer with the help of an example.

Question 4. [5+5=10]

a. Explain different types of malware that can affect your computer or network.
b. Suppose your antivirus detected a malware on your computer. Describe some ways to analyse this malware.

Question 5. What connectivity technologies can be employed in the following use cases? Justify your answer: [5+5=10]

a. Sensors-based low-powered device to be used in Air Quality Monitoring.
b. Smartphone for music streaming and online video streaming.

Question 6. [6+5=11]

a. What are the different attacks that an attacker can perform in the following cases, and what defence mechanisms you can use to defend against these attacks, explain:
   i. Network packet
   ii. Target machine
b. Explain how a buffer overflow attack works. Write a code snippet in C programming for a buffer overflow attack.

Question 7. Answer the following questions in regard to control systems. [5+5=10]

a. What are AP&S and Risk?
b. What are the different types of vulnerabilities?