S-748

Total Pages : 5 **Roll No. ----------**

MIT(CS)-103/CEGCS-03

Cyber Attack and Counter Measures: User Perspective

(MSCCS/PGDCS/CEGCS)

1ST Semester, Examination 2022(Dec.)

Time: 2 Hours Max. Marks: 70

Note : This paper is of Seventy (70) marks divided into two (02) Sections A and B. Attempt the questions contained in these sections according to the detailed instructions given therein.

Section – A

(Long Answer – type questions)

Note: Section 'A' contains Five (05) long-answer-type questions of Nineteen (19) marks each. Learners are required to answer any two (02) questions only.

[2 x 19 = 38]

P.T.O.

Q.1. Discuss the following in detail along with the example of each: (3.8 Marks each, 3.8 x 5 = 19)

a. DNS

b. IP Address

c. POP3

d. IMAP

e. SMTP

Q.2. Discuss the following in detail: (Marks are mention against each question)

a. MS-CHAP. (6 Marks)

b. Extensible Authentication Protocol. (7 Marks)

c. RADIUS (6 Marks)

Q.3. Discuss the following in detail: (Marks are mention against each question)

a. Discuss Public Key Cryptography, and its various application in detail. (10 Marks)

b. Discuss various steps involved in forensic investigation. Discuss various forensic tools. (9 Marks)

Q.4. Discuss the following in detail: (Marks are mention against each question)

a. SDLC SPIRAL model in detail with design, stages, application, advantages and disadvantages etc. (10 Marks)

b. SDLC V-Model in detail with design, stages, application, advantages and disadvantages etc. (9 Marks)

Q.5. Discuss the following in detail: (Marks are mention against each question)

a. Discuss Types of Authentication in detail. (10 Marks)

b. Discuss Software Prototyping Model in detail. (9 Marks)

Section – B

(Short-answer-type questions)

Note: Section 'B' contains Eight (08) short-answer-type questions of Eight (08) marks each. Learners are required to answer any Four (04) questions only.

[4 x 8 = 32]

P.T.O.

Q.1. Discuss WLAN, its various features and problems.

Q.2. Discuss Password Authentication Protocol.

Q.3. Discuss Big Bang Model.

Q.4. Discuss Authentication vs. Authorization in detail with diagram.

Q.5. Discuss Rapid Application Development (RAD) model in detail.

Q.6. Discuss cryptography? Discuss the objectives of cryptography? Discuss various types of crpytographic techniques?

Q.7. Discuss with examples:

a. SSL

b. Microsoft NTLM

c. Smart Cards

d. Biometrics

Q.8. Discuss with examples:

a. Protocols

b. Top-level domains

c. Second-level domains

d. Third-level domains

****