CEGCS–04

Information System

Certificate of E-Governance and Cyber Security

(CEGCS-16/17)

First Semester, Examination, 2018

Time : 3 Hours   **Max. Marks : 80**

Note : This paper is of **eighty (80)** marks containing **three (03)** Sections A, B and C. Learners are required to attempt the questions contained in these Sections according to the detailed instructions given therein.

Section–A

(Long Answer Type Questions)

Note : Section 'A' contains four (04) long answer type questions of nineteen (19) marks each. Learners are required to answer *two* (02) questions only.

1. Answer the following :

   (a) What do you understand by "impersonating the token" ? How does it help an attacker in escalating privileges ?   7

   (b) Explain the sequence of planting a backdoor using psexec utility.   7

   (c) How to bypass UAC Windows platform ?   5

2. Answer the following :

(a) Explain the difference between TCP and UDP. Which network applications you feel, these protocols are best suited for ?   9

(b) Explain the sequence of three-way handshake.   5

(c) Briefly explain the functioning of Internet e-Mail.

5

3. Explain the following :

(a) Hash algorithms.   7

(b) Symmetric encryption algorithms   6

(c) Asymmetric encryption algorithms   6

4. Answer the following:

(a) Explain Mouth Frog Protocol.   6

(b) Explain   Needham-Schroeder   Secret-Key Protocol.   7

(c) Explain Kerberos Protocol.   6

Section–B

(Short Answer Type Questions)

Note : Section 'B' contains eight (08) short answer type questions of eight (8) marks each. Learners are required to answer *four* (04) questions only.

1. What is NMAP ? Explain.

2. What do you understand by "Man in the middle attack" ? Explain briefly.

3. What are the basic five protections Cryptography can provide ? Explain.

4. Explain CIA triad.

5. What is hacking ? Explain the different types of hackers.

6. Answer the following :

    (a) What is the significance of key length ?

    (b) What are the two key criteria of a good hash function ?

7. Explain the process of Key Distribution Using Symmetric Key Protocols.

8. Discuss the strategy to improve crack resistivity of a key.

Section–C

(Objective Type Questions)

Note : Section 'C' contains ten (10) objective type questions of one (01) mark each. All the questions of this section are compulsory.

1. How to bypass UAC Windows platform ?

    (a) IP routing

    (b) RSA

    (c) NMAP

    (d) SNMAP

2. De facto standard for internetworking is .... Protocol.

    (a) ISO

    (b) TCP/IP

    (c) UDP

    (d) UIP

3. FQDN stands for ....

    (a) Fully Qualified Domain Name

    (b) Fully Queuing Domain Name

    (c) Functional Quality Distant Network

    (d) Frequently Qualified Domain Network

4. .... is a process for creating a unique digital fingerprint for a set of data.

    (a) Caching

    (b) Subnetting

    (c) Key distribution

    (d) Hashing

5. In computing, a .... attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

    (a) IP poisoning

    (b) Denial-of-Service (DoS)

    (c) Honeypot

    (d) RSA

6. A .... is a small-size datum from a block of digital data for the purpose of detecting errors which may have been introduced during its transmission or storage.

    (a) XSS

    (b) Cypher

    (c) Checksum

    (d) IP address

7. In a .... the cryptanalyst attempts every possible combination of key patterns.

   (a) Implementation attacks

   (b) Statistical attacks

   (c) Analytic attacks

   (d) Brute force attack (or exhaustion)

8. .... is an IETF open standard for secure communications over public IP-based networks, such as the Internet.

   (a) SSL

   (b) TSL

   (c) Digital Certificate

   (d) Internet Protocol Security (IPSec)

9. SSL stands for ....

   (a) Super Secure Level

   (b) Security Setup Limitation

   (c) Secure Socket Layer

   (d) Secure Setup Layer

10. .... is a Bash script in BackTrack, which could be used for detecting load balancers.

   (a) Load balancer detector (lbd)

   (b) XPS

   (c) Ping

   (d) cmd