CEGCS-04/PGDCS-04

Information System

Certificate of E-Governance and Cyber Security/
P.G Diploma in Cyber Security (CEGCS-16/17/PGDCS-17)

First Semester Examination, 2019 (June)

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

Note : This paper is of Eighty (80) marks divided into three (03) sections A, B and C. 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 any two (02) questions only.

(2×19=38)

1. Answer the following.

(a) Discuss the implementation of kerberos for key distribution? (6)

(b) Explain the process of key generation. (6)

(c) What should be the best strategy for key distribution and management in an organization? (7)

2. Define the following:

    (a) What is zone transfer? (6)

    (b) How this vulnerability can be misused by a hacker ? (6)

    (c) What is the remedial action one must take to mitigate this? (7)

3. Answer the following:

    (a) Explain Symmetric cryptographic algorithms. How it work? (6)

    (b) Explain Asymmetric cryptographic algorithms. How it works? (7)

    (c) Define digital certificate and it's working. (7)

4. Write a short note on the following:

    (a) IP subnetting. (3)

    (b) Post Office Protocol(POP3). (3)

    (c) Internet Message Access Protocol (IMAP). (4)

    (d) File Transfer protocol (FTP). (3)

    (e) Secure Socket Layer (SSL). (3)

    (f) HTTPS. (3)

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.   (4×8=32)

1. Answer the following:

   (a) What is port scanning?   (3)

   (b) What are the different types of port scanning techniques?   (5)

2. What is a trust Model?Explain Hiererchical Trust Model, Distributed Trust Model and Bridge Trust Model in details.

3. Explain TCP/IP architecture in details.

4. Explain CIA triad. What are the activities which break the CIA triad ?

5. What is hacking ? Explain the different types of hackers based on their intention.

6. Explain the different phases of PAN testing in details.

7. Answer the following:

    (a) What do you anderstand by Rainbow tables?   (4)

    (b) What is privilege escalation?   (4)

8. What do we understand by active and passive attacks? What are the various techniques used for carrying out these attacks?

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.   (10×1=10)

1. An _____ attack uses algebraic manipulation in an attempt to reduce the complexity of the algorithm.

    (a) Analytic

    (b) Brute force

    (c) Implementation

    (d) Statistical

2. _____ command will list all the interfaces, the IP addresses, gateway, and the MAC addresses.

   (a) arp-a

   (b) netstart

   (c) tasklist

   (d) ipconfig

3. _____ is digital certificate management.

   (a) MKI

   (b) PKI

   (c) TPM

   (d) HSM

4. A_____ policy is a published set of rules that govern the operation of a PKI.

   (a) Computer

   (b) Security

   (c) Ethics

   (d) Certificate

5. A_____ is a system or resource that is being evaluated for vulnerabilities.

   (a) Hack value

   (b) Target of Evalution

(c) Exploit

(d) Threat

6. _____ is the act of performing several hacking attacks in sequence with each building on or acting on the results of the previous action.

(a) Hack value

(b) Target of Evaluation

(c) Daisy Chaining

(d) Vulnerability

7. ARP stand for _____.

(a) Activity Recording Procedure

(b) Address Resolution Protocol

(c) Activity Resolution Procedure

(d) Activate Residing Program

8. In cryptography, a _____ is a method of encryption by which the positions held by units of plaintext are shifted according to a regular system.

(a) Transposition cipher

(b) Rail Fence cipher

(c) Route cipher

(d) Columnar transposition

9. _____ is the science of transforming information into a secure form so that it can be transmitted or stored and unauthorized persons cannot access it.

(a). Caligraphy

(b) Stegnigraphy

(c) Cryptography

(d) Digital signature

10. _____ is a function which delivers the kry to two parties who wish to exchange data securely

(a) Key generation

(b) Key storage

(c) Key distribution

(d) Key Utilization

———————