

CEGCS-03/PGDCS-03

Cyber Attacks and Counter Measures: User Perspective

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.** What is Information security ? What information Security controls can be employed to mitigate Cyber attack?
- 2.** What are the various categories of Computer Security controls? Enumerate all of them and discuss physical controls in detail.

3. Explain Challenge Handshake Authentication Protocol (CHAP) process in detail?
4. What is PKI ? How does it function? Discuss Three applications of this method of encryption.

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. Write short notes on following:
 - (a) Discretionary Access Control (DAC)
 - (b) Mandatory Access Control (MAC)
 - (c) Role Based Access Control (RBAC).
2. Write short notes on following:
 - (a) Software as a Service (SaaS)
 - (b) Platform as a Service (IaaS)
 - (c) Infrastructure as a Service (IaaS).
3. Compare the Information Security standards ISO 27001:2005 and ISO 27001:2013.
4. What are the three master categories into which computer Security is categorised?

5. What is software development and life cycle?
6. What are the best practices to ensure protection from malicious attacks?
7. What is an Intrusion Detection System? Explain its functioning?
8. What do you understand by risk management process in relation to Information Security? Enumerate the activities involved in Risk Management Process.

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)

State whether following statements are true or false :

1. SaaS, PaaS, and IaaS are the kind of cyber attack.
2. In asymmetric key cryptography, the private key is kept by sender.
3. Controls that substitute for the loss of primary controls and mitigate risk down to an acceptable level.
4. A security event that compromises the confidentiality, integrity, or availability of an information asset.

5. Software as service is a part of cloud computing.
 6. Software development lifecycle is essential process of encryption method.
 7. Authentication identify actual user while logging-in a particular website.
 8. Procedures implemented to define the roles, responsibilities, policies, and administrative needed to manage the control environment.
 9. Computer Worms are among the most common type of malware.
 10. Spoof E-Mail is also called Spam.
-