Total No. of Pages : 4 Roll No. .....

PGDCS-07
Advanced Cyber Security Techniques
PG Diploma in Cyber Security (PGDCS-17)
2nd Semester
Examination-2019

Time : **3** *Hours* *[Maximum Marks : 80*

Note : This paper is of Eighty (80) 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 Fifteen (15) marks each. Learners are required to answer any three (03) questions only. **(3×15=45)**

1. What do you mean by infrastructure security? Why maintenance, Monitoring and Analysis of Complete Audit Logs is critical control?

2. What is Cryptography? Explain how cryptography services have been leveraged in implementing a security layer over the traditional internet protocols?

3. What are MACRO's in the context of office applications. Explain in details which kind of threats they pose?

4. What is Indicators of Compromise (IOC)? Explain in detail the possible IOC from a preliminary static analysis?

5. (a) What is signature based detection? How it is different from anomaly detection? (8 marks)

   (b) Discuss HONEYPOT technology & its applications. (7 marks)

Section–B

(Short-Answer-Type Questions)

Note : Section 'B' contains Eight (08) short-answer-type questions of Seven (07) marks each. Learners are required to answer any Five (05) questions only. **(5×7=35)**

1. Discuss common controls to protect ICT from Fire disaster.
2. How to apply ACL on a file on both windows and Linux platforms?
3. Explain Defense in Depth approach?
4. Explain five common web applications attack.
5. Explain the procedure of enabling basic security in your desktop.
6. List out some of the advantage of Wireless LAN over Wired networks?
7. What is fuzzy hashing? HOW SSDEEP being advantageous over md5hash sum?
8. (a) Write a note on TIA-942 standard.

   (b) What is data center security ?