MIT (CS)-203/PGDCS-07
ADVANCED CYBER SECURITY TECHNIQUES

P.G. Diploma in Cyber Security (PGDCS-17)

2nd Semester, Examination-2020

Time Allowed : 2 Hours   Maximum Marks : 80

Note : This paper is of Eighty (80) marks divided into Two (02) sections A and B. Attempt the question 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 Twenty (20) marks each. Learners are required to answer any two (02) questions only.   (2×20=40)

1. What do you understand by Network Security? Discuss in detail about emerging threats to Cloud Computing and Internet of things.

2. What is log management in Network security? How it is different from security information and event management. Explain.

3. What do you understand by Secure Network Engineering? Discuss importance of Penetration Tests and Red Team Exercises.

4. What is Pretty Good Privacy? Explain the working of Pretty Good Privacy in detail.

5. (a) Write a short note on network Security technologies.

   (b) What is the difference between network based and host based intrusion detection and prevention system.

Section-B

(Short answer type questions)

Note: Section-B Contains Eight (08) short answer type questions of Ten (10) marks each. Learners are required to answer any four (04) questions only.   (4×10=40)

1. Write about five common attacks possible on computer networks with examples.

2. What is a Honeypot? Discuss different type of Honeypots.

3. What is a firewall? Discuss different type of firewall filtering.

4. Explain the role of Domain Name System Security Extension in Network Security.

5. Write note on SANS Critical controls for cyber defence.

6. Discuss emerging threats to cloud computing and Internet of Things (I.T).

7. Define BYOD and its associated security risks.

8. Explain Dan Kaminsky's DNS cache poisoning.

****