Roll No. | | | | | | | | | | | | Total No. of Pages : 01

Total No. of Questions : 08

M.Tech. (IT) PT (Sem.–5)

INTRUSION DETECTION AND ANALYSIS

Subject Code : MTIT-303

M.Code : 74154

Time : 3 Hrs. Max. Marks : 100

INSTRUCTIONS TO CANDIDATES :

1. Attempt any FIVE questions out of EIGHT question.
2. Each question carry TWENTY marks.

1. Justify the need of an efficient intrusion detection system. What are the major challenges for an intrusion detection system?
2. What are the key functions of intrusion detection system? Explain few common methodologies for intrusion detection.
3. Explain the flow process for Snort and Bro. Analyze the difference and similarities in Snort and Bro.
4. What are the five most prominent business security issues in a networked environment? Explain possible methods to tackle each one of them.
5. What is firewall? What are different categories of Firewall Policies? Give at least five different example of firewall configurations.
6. Write detailed note on any two of the following :

   a) Signature-based detection and anomaly-based detection.

   b) Differences between intrusion detection system and firewall.

   c) Honeypots.
7. What is malware? How malware may affect the security of the system? Explain some of the anti-malware technologies available.
8. Suppose you are a security analyst and network administrator of an organization. The financial transactions of the organization are under continuous threat of breach. What strategy you will follow to analyze the threat level and propose a security solution to the organization? Give a detailed solution with proper justification.

NOTE : Disclosure of Identity by writing Mobile No. or Making of passing request on any page of Answer Sheet will lead to UMC against the Student.