Course Code: MCA-253 Course Name: Cyber Security and Cyber Laws

**Assignment - 2**

(Based on Unit – III)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | | | |  |
| Sr. No. | | **Question** | BTL | CO | Marks | | |
| 1 | | With the vast expansion of computer network usage and the vast expansion of the number of applications operating on top of it, network secrecy is growing in significance. All computer systems are susceptible to security flaws that are both technically and economically challenging for manufacturers to fix. Consequently, the importance of Intrusion Detection Systems (IDSs) as devices designed to detect network anomalies and intrusions is growing.  Long ago, the majority of intrusion detection research was devoted to anomaly-based and misuse-based detection techniques. In commercial products, misuse-based detection is typically favoured due to its predictability and high accuracy. However, in academic research, anomaly detection is regarded as a more potent technique due to its theoretical capacity to combat novel attacks.  Several machine learning methods are reported to have a very high detection rate of 98% while maintaining a false alarm rate of only 1%, according to a comprehensive analysis of the recent research trend in anomaly detection. However, when examining the most advanced IDS solutions and commercial tools, there is no evidence of the use of anomaly detection approaches, and practitioners continue to view the technology as infantile. To determine the cause of this disparity, a great deal of research has been conducted on anomaly detection, focusing on various aspects including learning and detection approaches, training and testing data sets, and evaluation techniques.  Build network intrusion detection system to detect anamolies and attacks in the network. There are two problems.   1. Binomial Classification: Activity is normal or attack 2. Multinomial classification: Activity is normal or DOS or PROBE   This data is KDDCUP’99 data set, which is widely used as one of the few publicly available data sets for network-based anomaly detection systems.  For more about data: <http://www.unb.ca/cic/datasets/nsl.html> | BTL6 | CO4 | 25 | | |
|  | |  | | | | |  |
|  | |  | | | | |  |
|  | |  | | | | |  |
|  | |  | | | | |  |
|  | |  | | | | |  |
|  | |  | | | | |  |