Type of Attack in Computer Network using Intrusion Detection System with Data Mining techniques – A Survey

Mr. Balram Purswani
Ph.D. Scholar
Mewar University
Chittorgarh (Rajashthan)

Dr. Samar Upadhyay,
Head Computer Applicaion,
Government Engg. College,
Jabalpur(M.P.)India 482001

Abstract

An **Intrusion Detection System** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a anagement station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization. They search for potential malicious abnormal activities on the network traffics; they sometimes succeed to find true network attacks and anomalies (true positive). However, in many cases, systems fail to detect malicious network behaviors (false negative) or they fire alarms when nothing wrong in the network (false positive). Hence applying Data Mining (DM) techniques on the network traffic data is a potential solution that helps in design and develop a better efficient intrusion detection systems. Data mining methods have been used build automatic intrusion detection systems. The central idea is to utilize auditing programs to extract set of features that describe each network connection or session, and apply data mining programs to learn that capture intrusive and non-intrusive behavior. In addition, Network Performance Analysis (NPA) is also an effective methodology to be applied for intrusion detection. Here, we discuss DM and NPA Techniques for network intrusion detection and propose that an integration of both approaches have the potential to detect intrusions in networks more effectively and increases accuracy .

Keywords *: Intrusion Detection, Network Intrusion Detection System, Data Mining Techniques, Network Performance Analysis.*