Abstract

Denial of Service attacks are the most common attacks prevailing in the vast field of networking now a days, the other three being the User-to-root, Remote-to-Local and Probe attacks. There are again a number of attack modes existing from each of these four classes. Anomaly detection, detection of deviations from what is considered normal, is an important complement to misuse detection based on attack signatures. In this paper, we discuss TCP Syn Flooding attack is discussed, the most common among the denial of service attacks, along with its basics, its affects, its detection and the different existing algorithms to serve as its remedies. The various preprocessed and header based parameters can be successfully used to detect this attack. Various features are extracted from the traffic captured. Header based features, content based features, time based features and connection based features are used to prepare various datasets for performing classification analysis. Unsupervised and supervised classification algorithms are then applied for classifying the data.