ABSTRACT

Port scanning, a favourite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. It is one of the most fundamental techniques that a hacker can use to begin an attack. Co-ordinated scanning is the use of multiple hosts in scanning. Similar to slow scanning, this spreads the suspicious activity of a scan over multiple source IP addresses as target sockets are divided among scanners. Due to lack of availability of labelled datasets for training or validation of the models, most of scan detection approaches result with high false alarms that requires attention. In this project we have generated our own dataset by generating co-ordinated port scans on fully dedicated machines, capturing the packets and extracting the interesting features.

Further, we have tried to develop a supervised method for classifying an Intrusion Dataset, and we tested the method on an already existing standard dataset – the KDD Cup Dataset. Also, we have suggested an improvement in the generic architecture of an Intrusion Detection System. Finally, we made a comparative study of the performance of our method with existing standard algorithms like K-means clustering and C4.5 Decision tree.