

CONCLUSION

The proposed mechanism eliminates the need for a Signature Based System of detection. The advantage of not depending on a Signature Based System is that we can easily detect novelty attacks. The proposed system protects the network by constantly monitoring the TCP flags and checking for outliers. It alerts the administrator whenever in an attack state. The Naive Bayes Classifier which is implemented in this project is a “site-based”, real-time system which is simplistic in its design and deployment. Successful testing on standard datasets such as the DARPA dataset, KDD dataset and the AUCKLAND-II dataset with accuracies over 95% has proved the project to be a success. The proposed mechanism can also be applied for other flag based protocols like the User Datagram Protocol. The Naive Bayes Classifier has successfully detected and alerted the administrator of a Distributed Denial of Service attack.

The accuracy of the system is calculated based on False Positives (FP) and False Negatives when tested against “No Attack” files and “Attack” files. The system has two operational phases; 1. Training Phase and 2. Testing Phase. A normal profile of the network is generated during the Training Phase. The Testing Phase is then started by using an attack file. Based on the threshold probability obtained during the training phase, incoming packets are classified as an attack or a non-attack packet. Finally, we have tested the system with three standard datasets, i.e DARPA, KDD and AUCKLAND-II with satisfactory results.

The proposed system has the following outcomes:

- A systems approach for DoS and DDoS detection at target using a Naive Bayes Classifier for TCP, with a design engineered for real time use and implement-ability.
- Design considerations taking into mind practical user problems with machine learning techniques.
- Light weight detection algorithm, with a note on processing latency and reaction time.