Abstract

The traditional approach for detecting novel attacks in network traffic is to model the normal frequency of session IP addresses and server port usage and to signal unusual combinations of these attributes as suspicious. Rather than just modeling user behavior, recent systems model network protocols from the data link through the application layer in order to detect attacks that
exploit vulnerabilities in the implementation of these protocols. We describe modular approach for network anomaly detection. Our system analyses the network traffic at three different possible levels (packet, flow, protocol) with the help of three different modules. Total anomaly score is computed from the anomaly scores of the three modules using weighted attribute model. We detect 147 of 185 attacks in the DARPA off-line intrusion detection evaluation data set [1] at 10 false alarms per day (total 100 false alarms), after training on one week of attack-free traffic. We investigate the performance of the system when attack free training data is not available.

Reference

- Ptacek, Thomas H., and Timothy N. Newsham, "Insertion, Evasion, and Denial of
Hybrid Modular Approach for Anomaly Detection System


Index Terms

Computer Science  Network Security

Key words

Hybrid  Anomaly Detection  DARPA