Team 05 - ISCXIDS2012 Dataset Abstract

One of the major challenges of the information age, has been finding efficient and cost effective ways to protect against or mitigate cyberattacks against network infrastructure. Intrusion detection systems can serve as an effective way to alert information security professionals of potential attacks against a network. Our team has devised a machine learning model using the random forest method to identify normal and malicious traffic based on the ISCXIDS2012 dataset. The model splits the dataset into multiple training sets, and compares the normal and attack traffic in order to train the model to evaluate network traffic. In addition, using information from the data set we have performed an in depth analysis of the network traffic, providing visualizations on the most common ports, protocols, and applications used, as well as the attack vectors identified. Using the Lockheed Martin cyber kill chain framework we have mapped some network traffic to what we believe are different stages within the kill chain. With conclusions from the analysis we have identified several potential vulnerabilities with certain protocols and ports in use. In an effort to reduce risk we have provided policy recommendations to eliminate vulnerable protocols as well as other recommendations we believe would mitigate or even prevent cyber attacks against this network.