KHIZR ALI PARDHAN | 301314376 | GITHUB.COM/ALIK604

CO-OP AT THALES CANADA

12/9/2019

Khizr Ali Pardhan | 301314376 | github.com/alik604
Co-op at Thales Canada

Design your own project – learnings in cybersecurity

My project consists of

- 4 pieces of code (+1 mini-project, bandwidth-hog, *Download a file many times, but do not save the data. Useful for stressing out a network... possibly your own)*
- Two blog posts
  - Blog post: Predicting the NSL-KDD Data Set with > 98% Accuracy
  - Blog post: Dimensionality Reduction — effects on model accuracy

Total time spend is about 60 hours, plus much more time for the prerequisite knowledge (very little is from my classes)

An introduction, not written by me (src),

> One of the major research challenges in this field is the unavailability of a comprehensive network based data set which can reflect modern network traffic scenarios, vast varieties of low footprint intrusions and depth structured information about the network traffic. Evaluating network intrusion detection systems research efforts, KDD98, KDDCUP99 and NSLKDD benchmark data sets were generated a decade ago.....This data set has a hybrid of the real modern normal and the contemporary synthesized attack activities of the network traffic. Existing and novel methods are utilised to generate the features of the UNSWNB15 data set

- KDD cup '99
  - 100% Accuracy
  - **Blog post**
- NSL-KDD (corrected dataset based off KDD cup '99')
  - 98% Accuracy
  - Affects of Dimensionality Reduction
  - **Blog post**
- UNSW_NB15
  - 92% Accuracy, with Ensemble (non neural network techniques; 'voting' on classification)
  - 91% Accuracy with feedforward neural network
- Anomaly Detection (Finance)
  - SPX 500 - pointing out oddities from the past and present
  - Exploring some elementary anomaly detection methods being applied to time series analytics

Sincerely,
Khizr Ali Pardhan | 301314376 | github.com/alik604
Information security analyst @ Thales Canada