Network Covert Channels Detection Using

Machine Learning

Project Brief Summary

**Project Title:** Network Covert Channels Detection Using Machine Learning

**Presented by:** Group#: IT02 (Terence Yu, Ambreen Zafar, Chetan Rajpal, Amad Mohamed)

**Supervised by:** Dr. Sk Md Mizanur Rahman

**Purpose:** Detection of covert channels to mitigate transmitted data from breaches

**Description:** This project created a tool for detecting covert channels in live networks through the use of machine learning.

Methodology involved the following:

* Researching and understanding into covert channels and machine learning
* Identifying, understanding, compiling, and running available tools used for generating covert data. The identified tools are *covert\_tcp* and *TunnelShell*.
* Generation of datasets for supervised learning composed of packets that contain covert channels and packets that do not.
* Testing of covert channel detection using 6 different binary classification machine learning algorithms: logistic regression, naive bayes, support vector machines, decision trees, k-nearest neighbors, and deep neural networks
* Generation of python code that can process packets, perform machine learning training and prediction, and detection of covert channels on live network

**Results:** Among the different machine learning algorithms tested, Decision Tree algorithm proved as the most effective in detection of covert channels. Conclusion is based on the algorithm providing the second best results in terms of precision, recall, and F1 score results while at the same time providing fast processing times and small model sizes.

Decision Tree algorithm results:

* Precision: 99.80%
* Recall: 99.96%
* F1: 99.88%
* Ave. processing time (200k records): 10,000 ms
* Model file size: 14kb

Covert-channel detector software is developed to use the model to detect covert channels in live packets.

|  |  |
| --- | --- |
|  |  |