Network Intrusion Detection

Geetesh Nikhade (gpn218), Rahul Keshwani (ryk248)

Background:

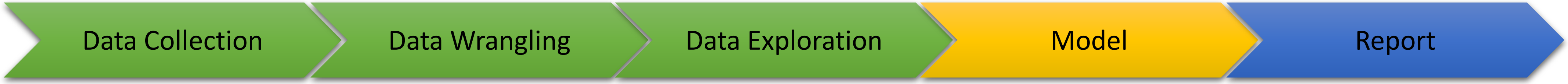
With the advent of IOT devices and network enabled systems, there is a dire need for smart firewalls and secure systems which can determine if the network and members connected to the current network are safe.

Goal:

a) Use an intelligent network intrusion detection system to classify if the incoming network packet is malicious/benign.

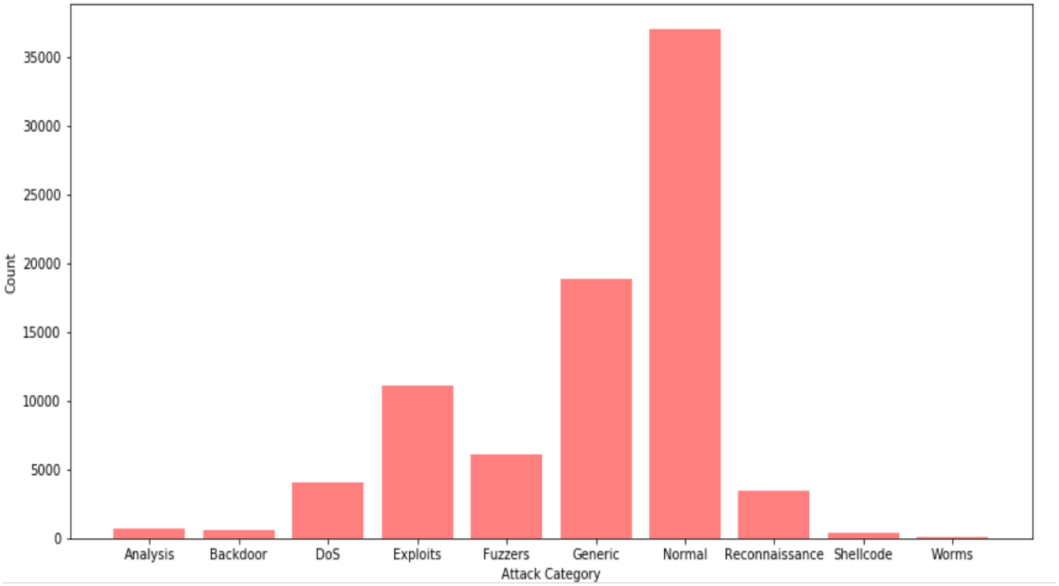
b) Determine the type of attack (e.g. DoS, Exploits, Fuzzers etc.)

Our Workflow:

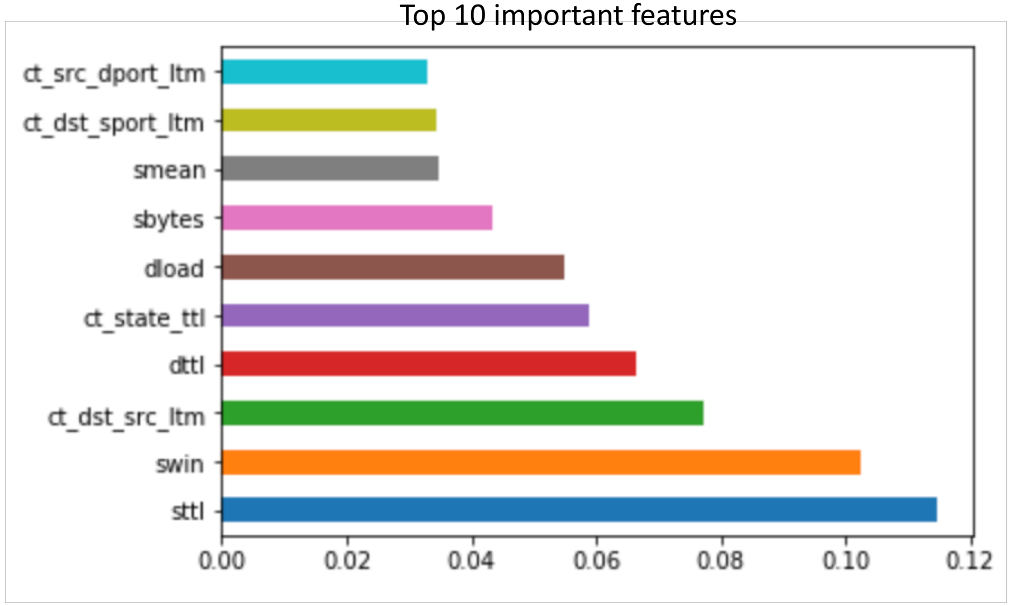


Data Collection → Data Wrangling → Data Exploration → Model → Report

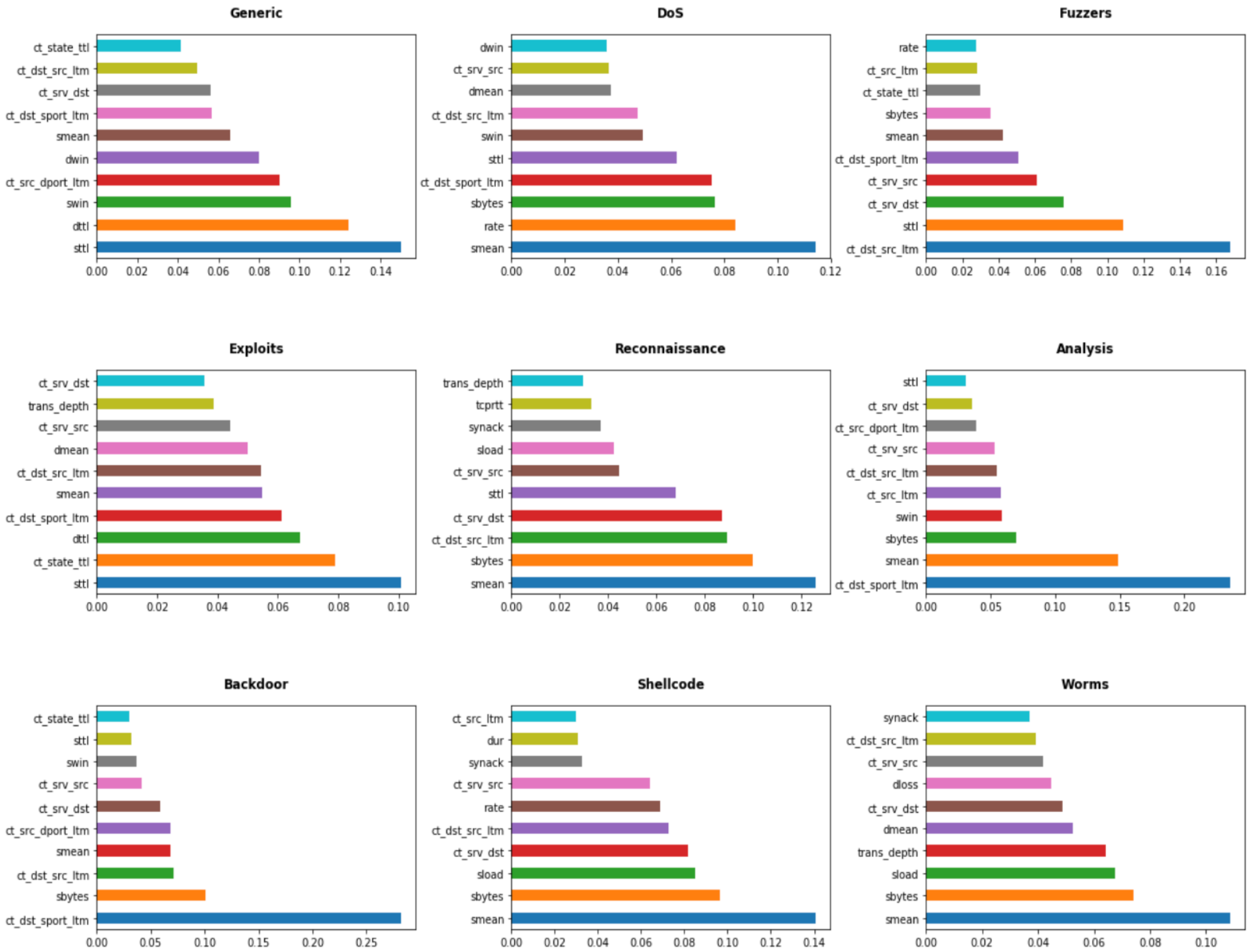
Distribution of attack types



Top 10 important features

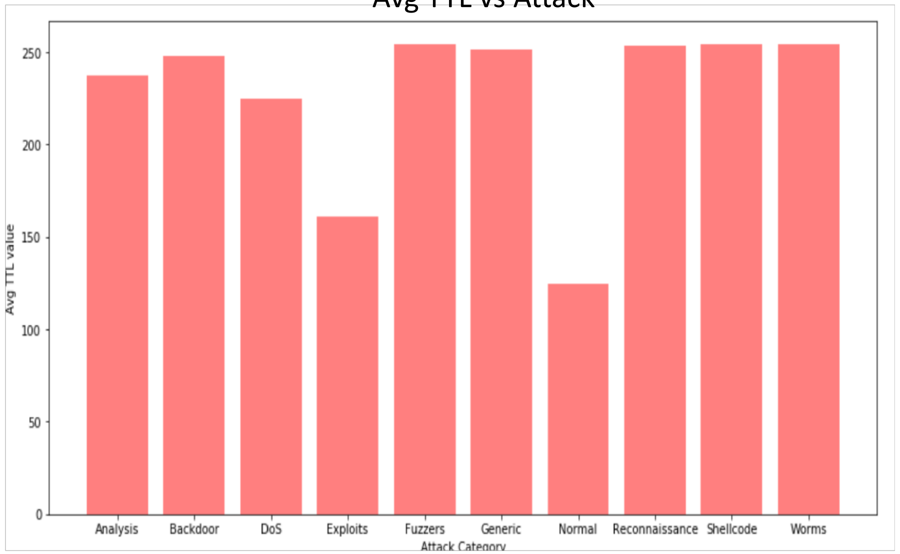


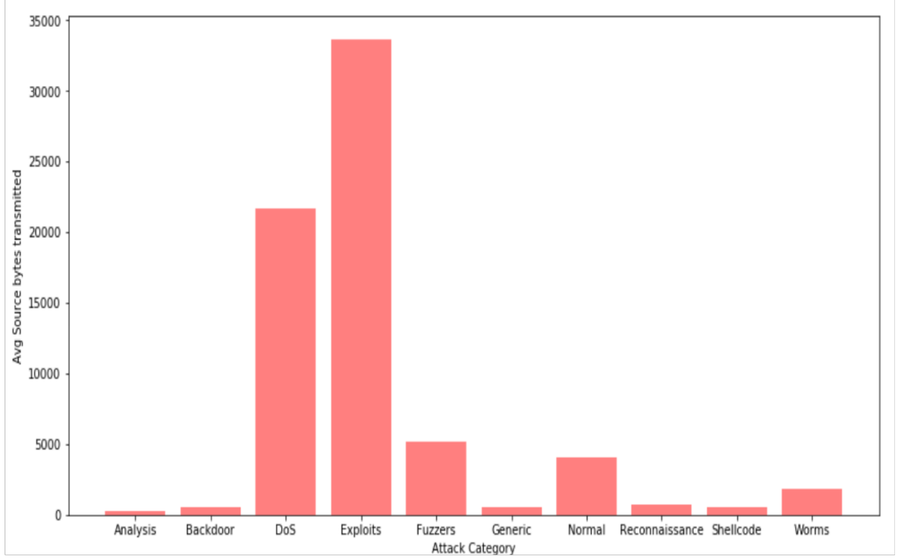
Exploratory Data Analysis



Top 10 features according to Attack type

Avg TTL vs Attack





Avg source bytes count vs Attack

Preliminary Model Results:

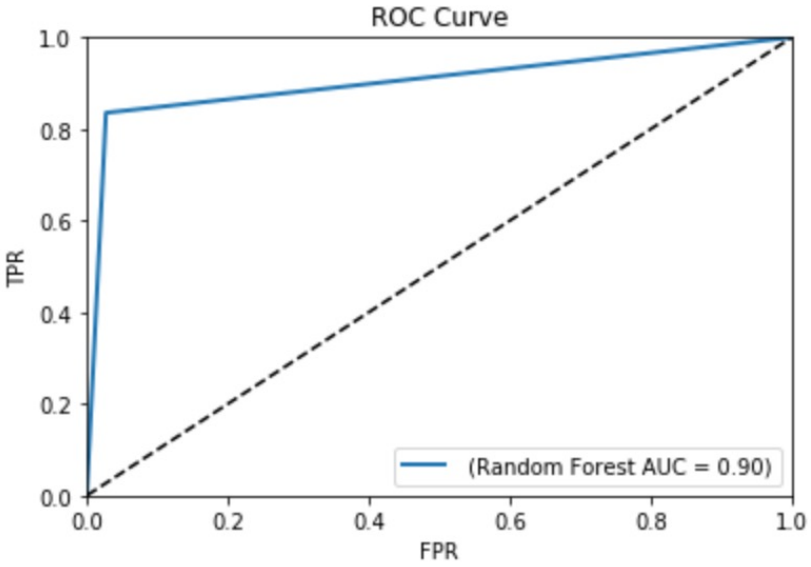
1. Confusion Matrix (Random Forest)

Prediction\Actual	Positive	Negative
Positive	99719	1525
Negative	19622	54475

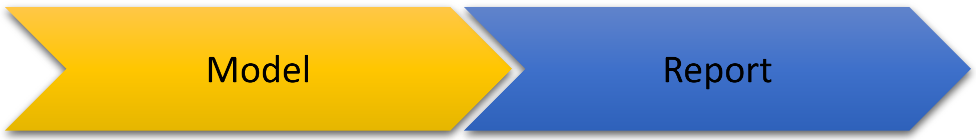
2. Evaluation Metrics (Random Forest)

Accuracy	Precision	Recall
87.94%	90.52%	87.94%

3. ROC (Random Forest)



Next Steps:


Model

Report

1) Perform PCA and build a Multi class classifier using Random Forest to further predict the attack category.

2) Build a boosting model (XGBoost) to perform both Binary and Multi class classification.

3) Create a detailed report presenting all the steps of our workflow.