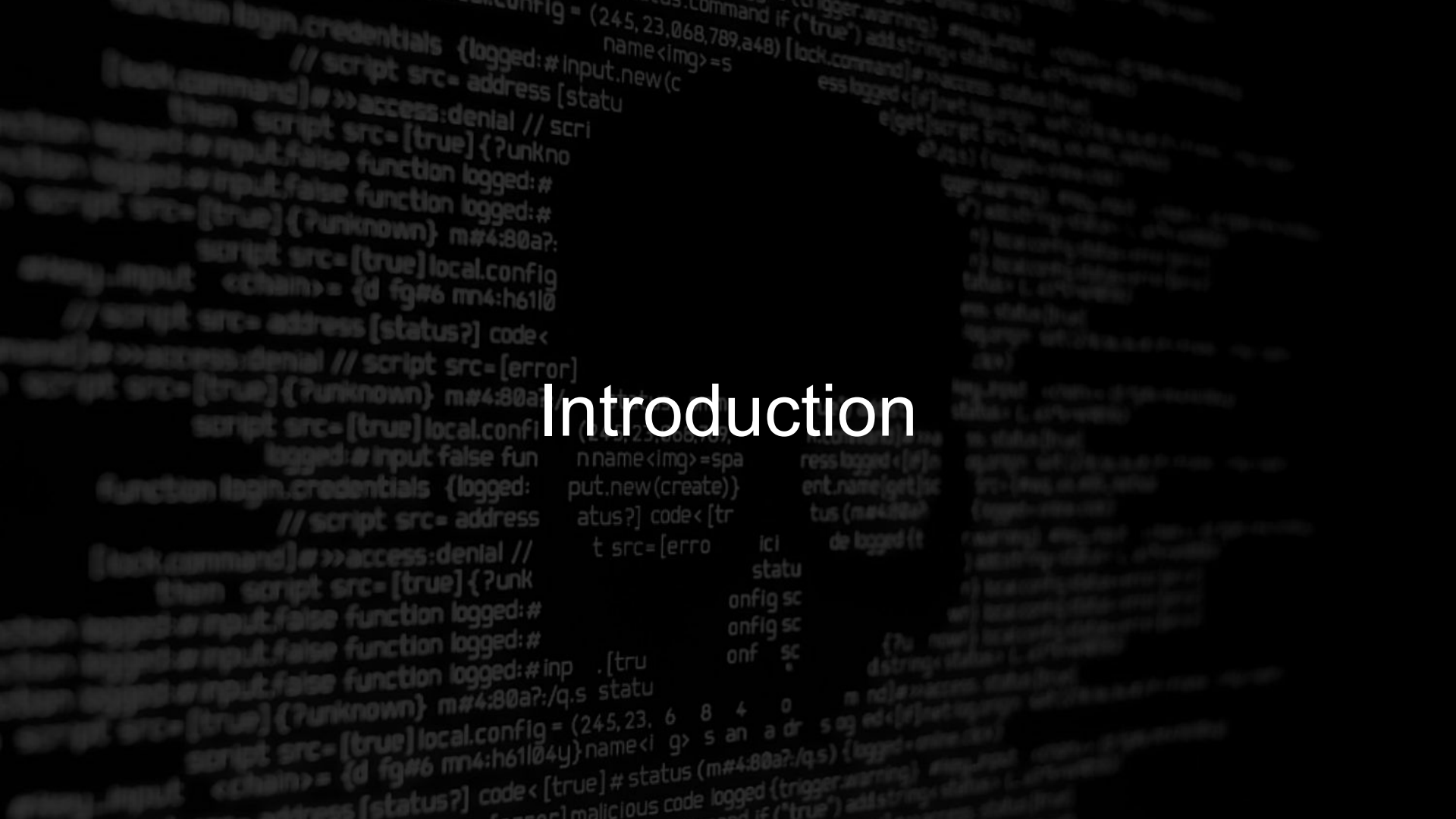
Mitigating DDoS Attacks and Ensuring Service Availability

Nate DiRenzo

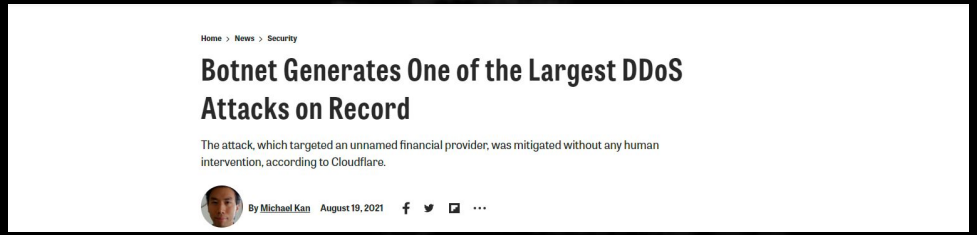
Agenda

- Introduction
- Business Problem
- Proposed Solution
- Success Metrics
- Data
- Model Selection & Results
- Conclusions
- Validation
- Further Work


Introduction

What is a DDoS attack?

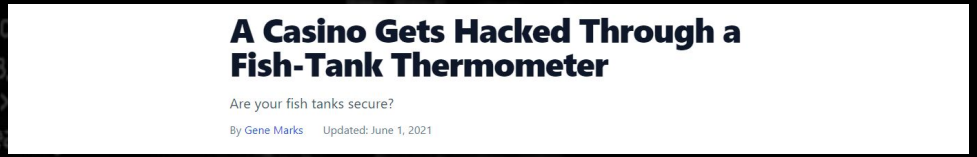
- Distributed Denial of Service (DDoS)
- Swamp a target service/network/infrastructure with junk traffic
- ‘Bots’ organized into ‘botnets’, directed by attacker
- Any internet-connected device can be compromised and co-opted


Home > News > Security

Botnet Generates One of the Largest DDoS Attacks on Record

The attack, which targeted an unnamed financial provider, was mitigated without any human intervention, according to Cloudflare.

By Michael Kan August 19, 2021


A Casino Gets Hacked Through a Fish-Tank Thermometer

Are your fish tanks secure?

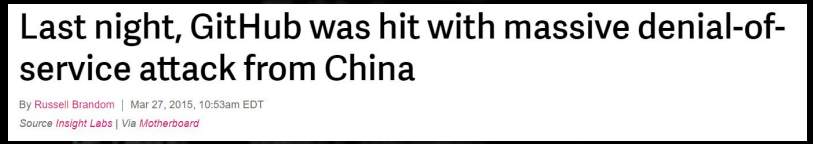
By Gene Marks Updated: June 1, 2021


'Smart' home devices used as weapons in website attack

22 October 2016

Why are DDoS attacks a problem worth solving?

- Directed at all industries
- For all kinds of reasons
- Inexpensive
- ‘Traditional’ DDoS damages
- Ransom, Extortion-based attacks
- More commonplace, evolving rapidly

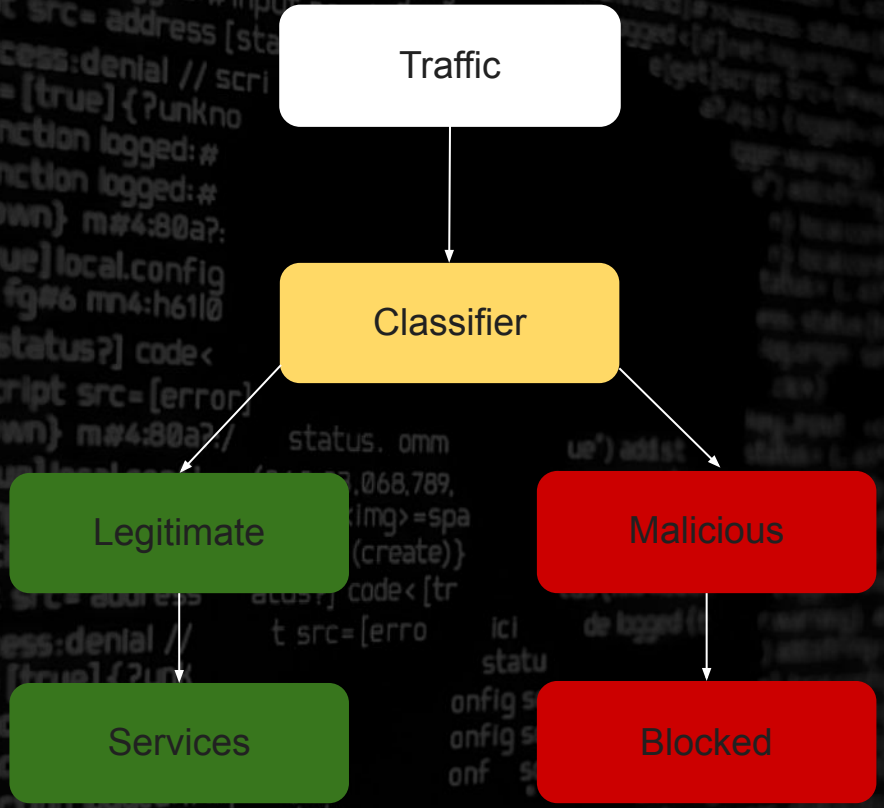



Business Problem

Mitigate the effects of a DDoS attack on business operations by identifying and blocking malicious traffic, thereby ensuring service availability for legitimate traffic.

Proposed Solution

Binary Classification Model



Success Metrics

Success Metrics

Business Terms:

- Minimize misidentification of legitimate traffic as malicious (ideally to **0**)
- Mitigate effects of DDoS attack by **90%**

Statistical Metrics:

- **Recall**: As close to **1.0** as possible
- **Precision**: Greater than or equal to **.9**
- $\mathbf{F_2}$: Optimizing metric for model selection


Data

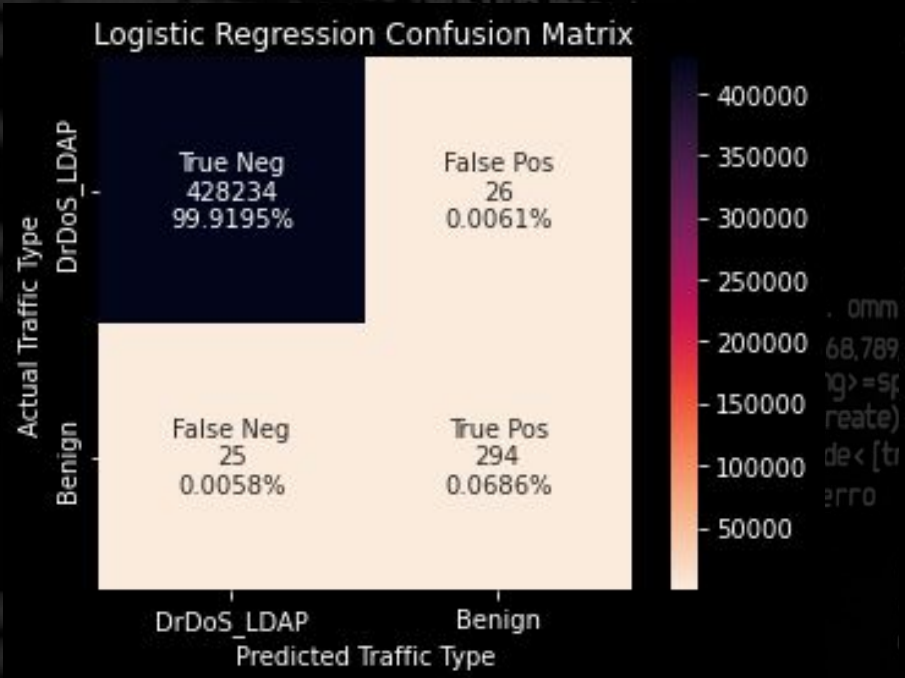
Data

- DDoS Evaluation Dataset CIC 2019
  - *With permission, Canadian Institute for Cybersecurity @ University of New Brunswick*
- Synthetic attack conducted using on-premise testbed with simulated benign interactions
- Dataset generated from .PCAP files containing packet information using CICFlowMeter
- 2,181,542 Observations
- 88 Features
- Heavily Imbalanced: 99.926% Malicious/0.073% Benign
- NaN/Infinity values dropped, traffic origination features removed
- Binary Labels
  - DrDoS_LDAP = Malicious
  - BENIGN = Legitimate

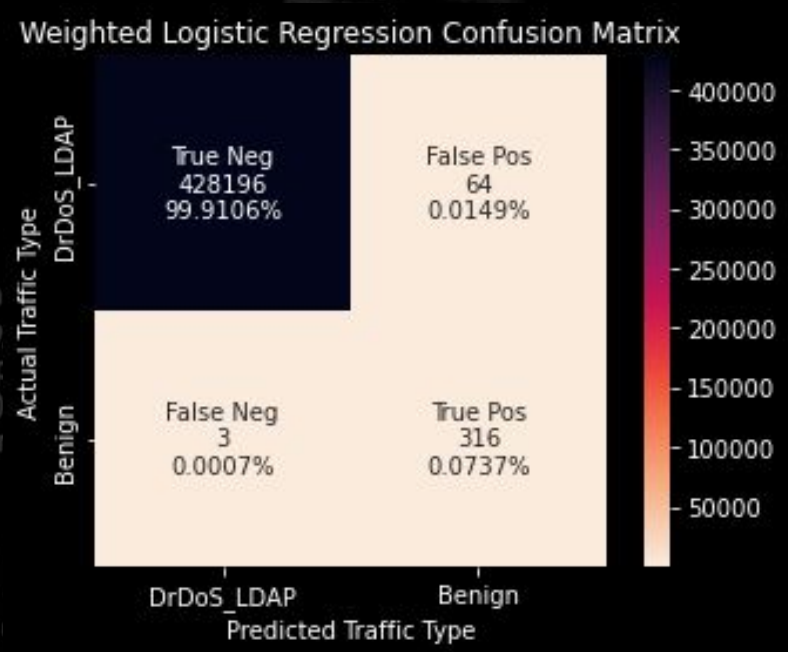
Model Selection & Results

Logistic Regression

Baseline Model



With Balanced Class Weights

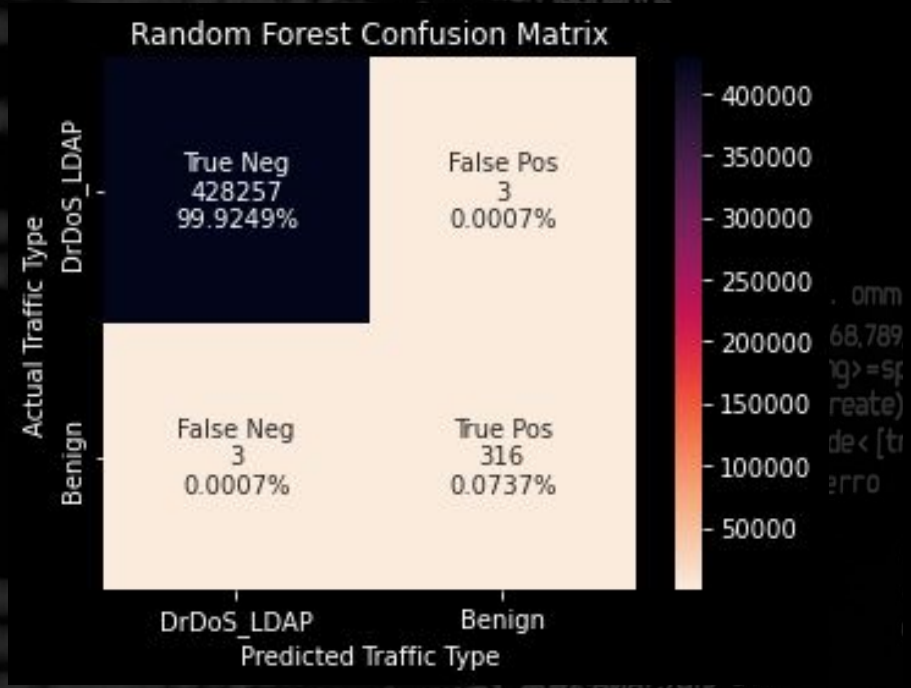


F_2: .921 Recall: .921 Precision: .918

F_2: .954 Recall: .990 Precision: .831

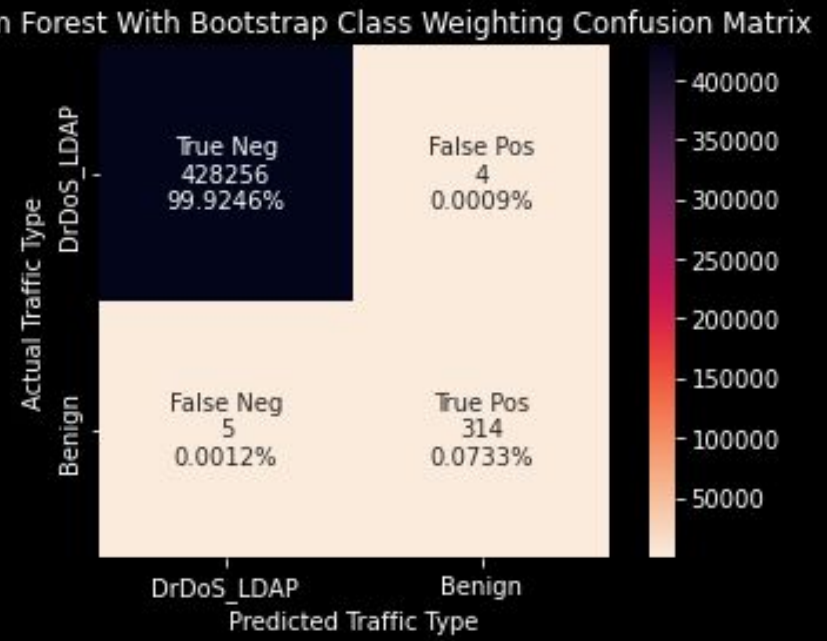
Random Forest

Baseline Model



F_2 : .990 Recall: .990 Precision: .990

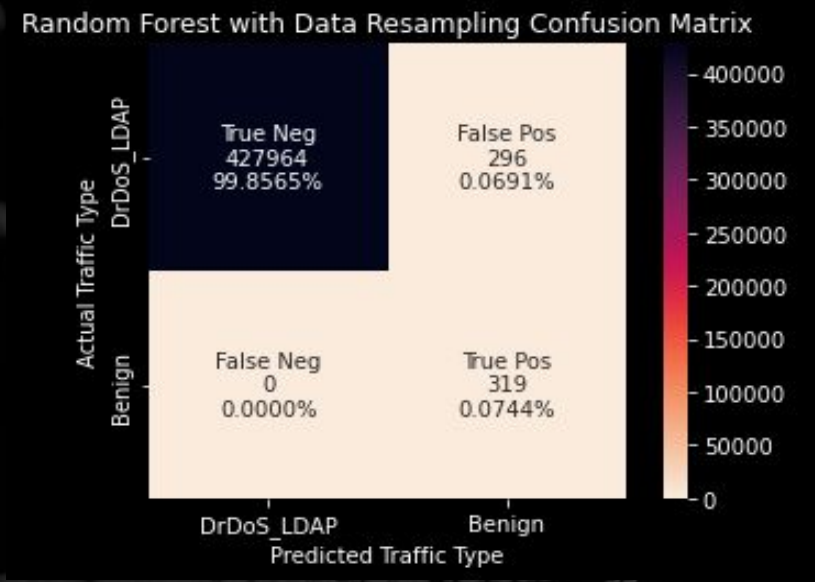
With Bootstrap Class Weighting



F_2 : .977 Recall: .974 Precision: .990

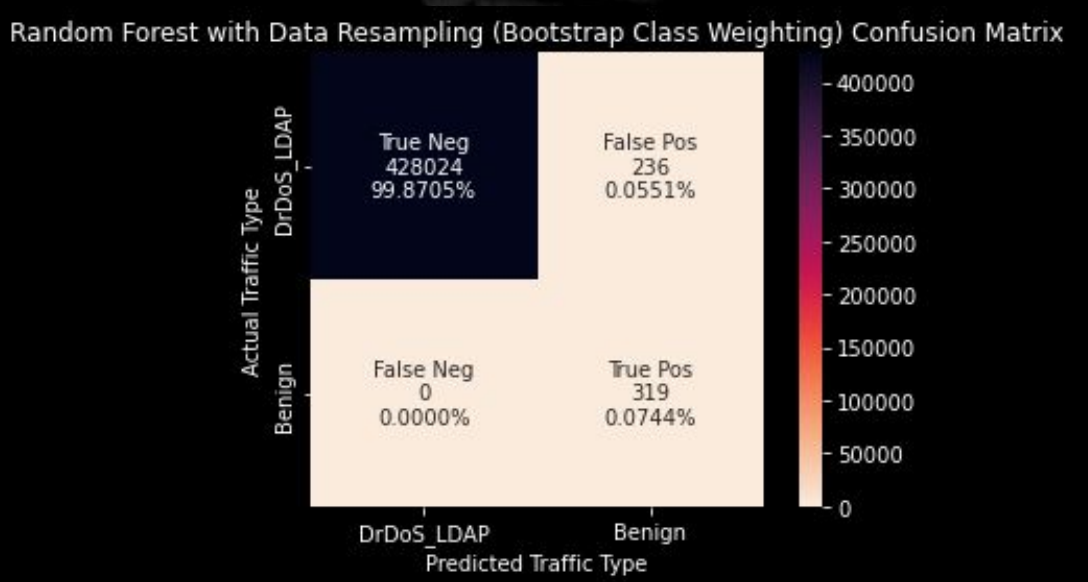
Imbalanced Random Forest

Baseline Model



F_2 : .984 Recall: .984 Precision: .987

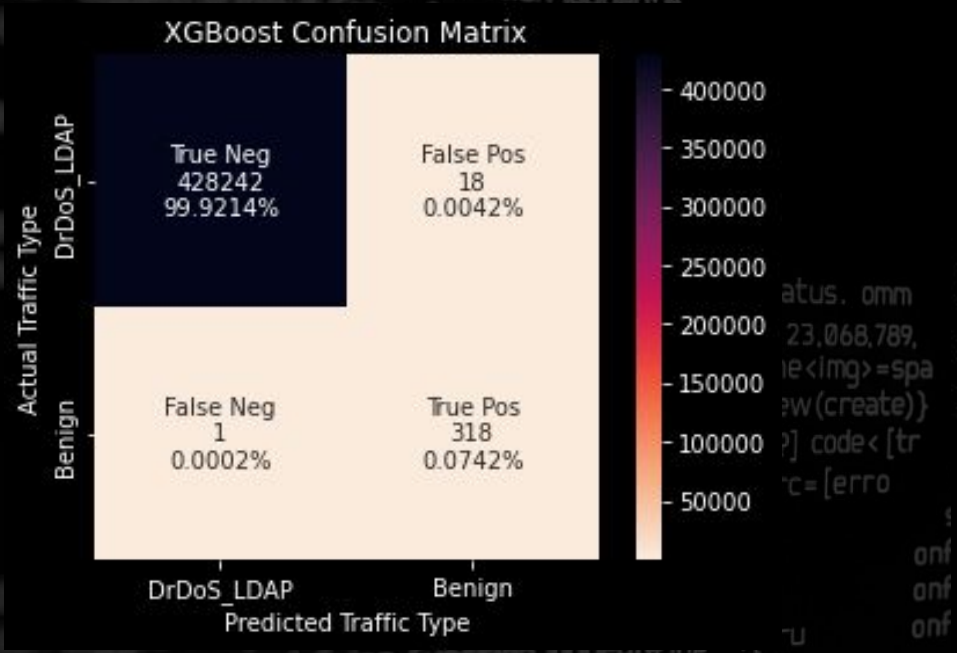
With Data Resampling & Bootstrap Class Weighting



F_2 : .871 Recall: 1 Precision: .574

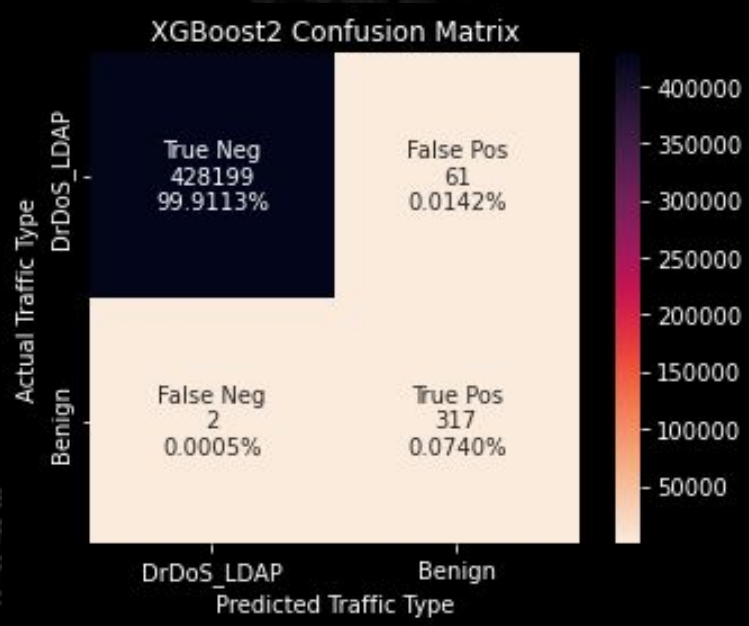
Gradient Boosted Trees (XGBoost)

Baseline Model



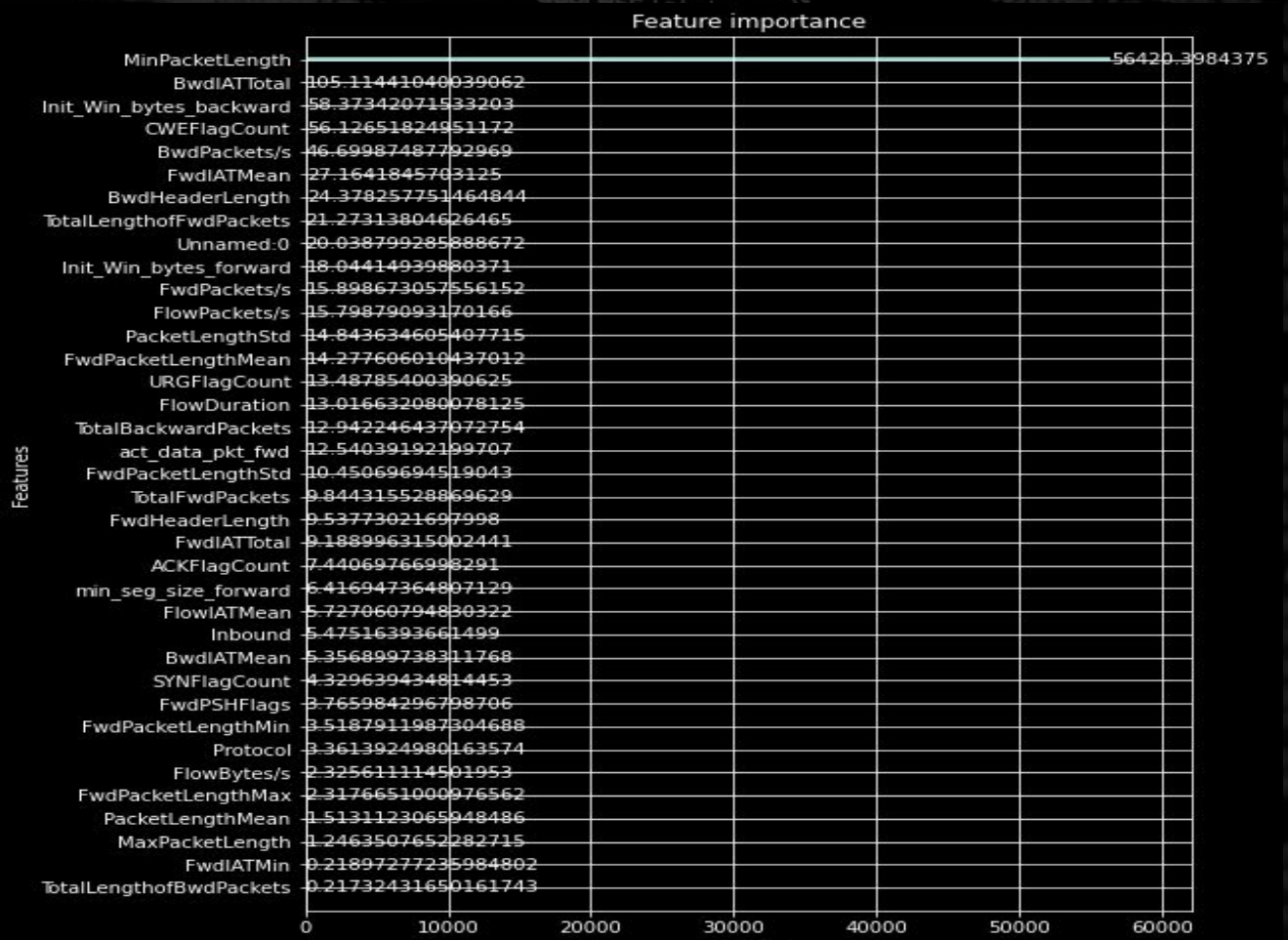
F_2 : .986 Recall: .996 Precision: .946

With Balanced Class Weights



F_2 : .958 Recall: .993 Precision: .838

XGBoost - Feature Importance by information gain



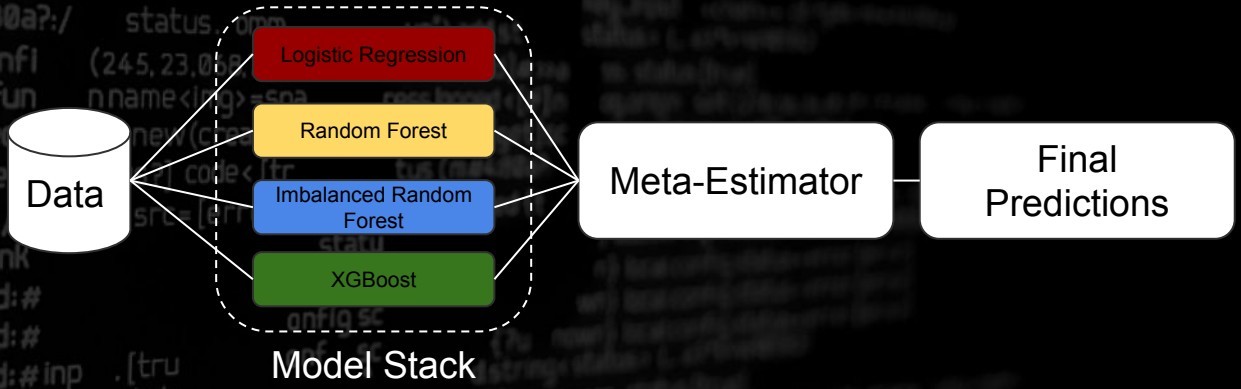
Ensembling

Final Models:

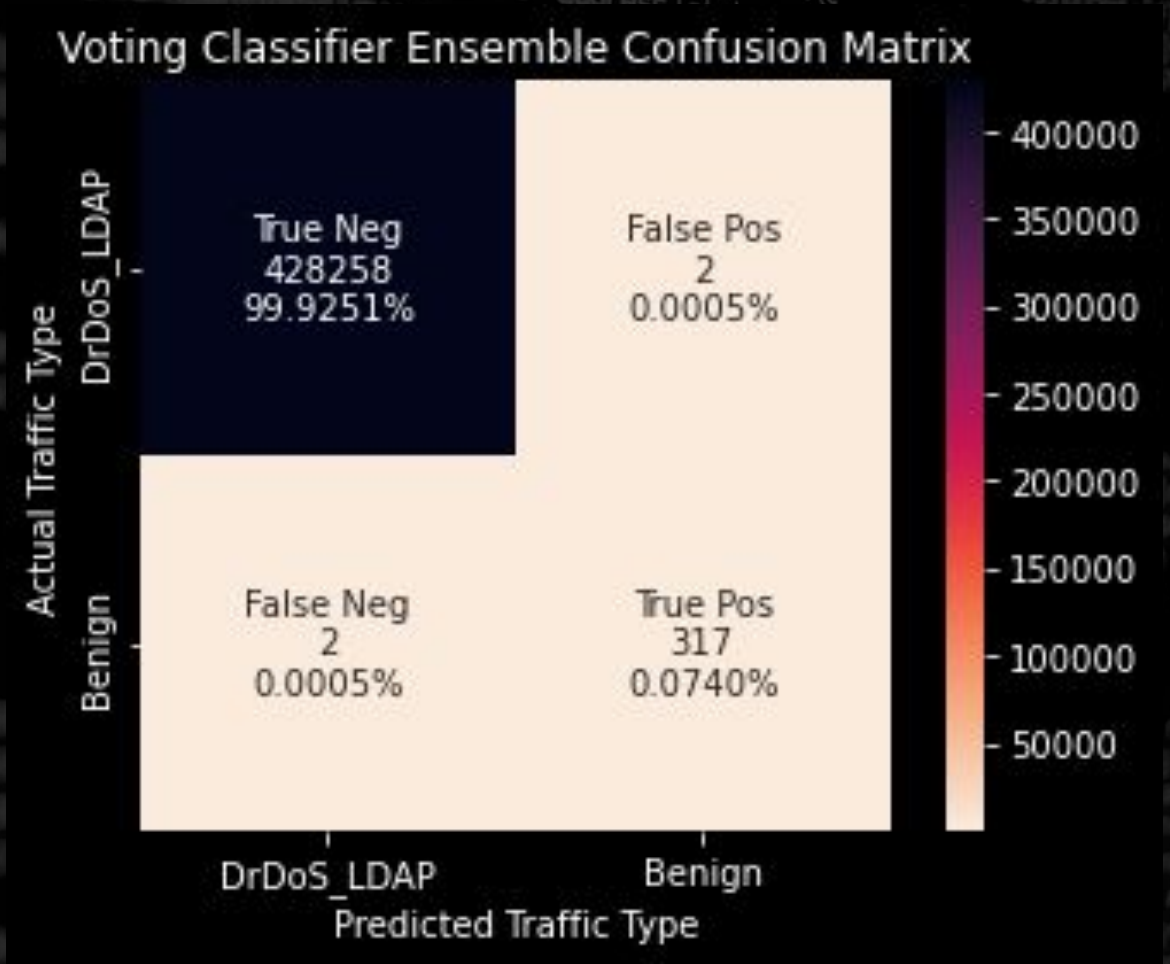
1. Weighted Logistic Regression
2. Baseline Random Forest
3. Imbalanced Random Forest with Bootstrap Class Weights
4. Baseline XGBoost

Methods Attempted:

1. Voting Classifier
2. Soft Voting Classifier
3. Stacked Classifier



Voting Classifier

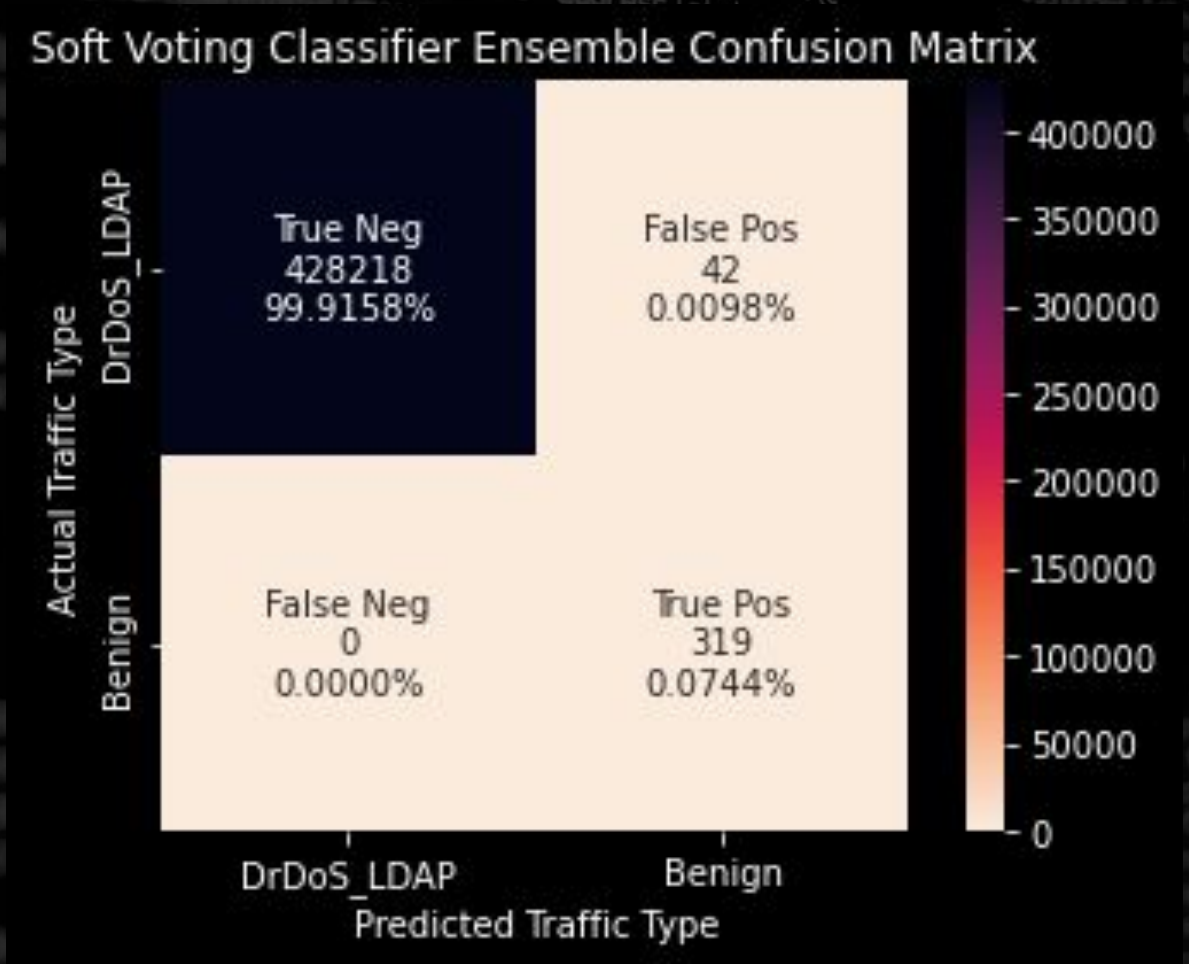


F_2 : .993

Recall: .993

Precision: .993

Soft Voting Classifier

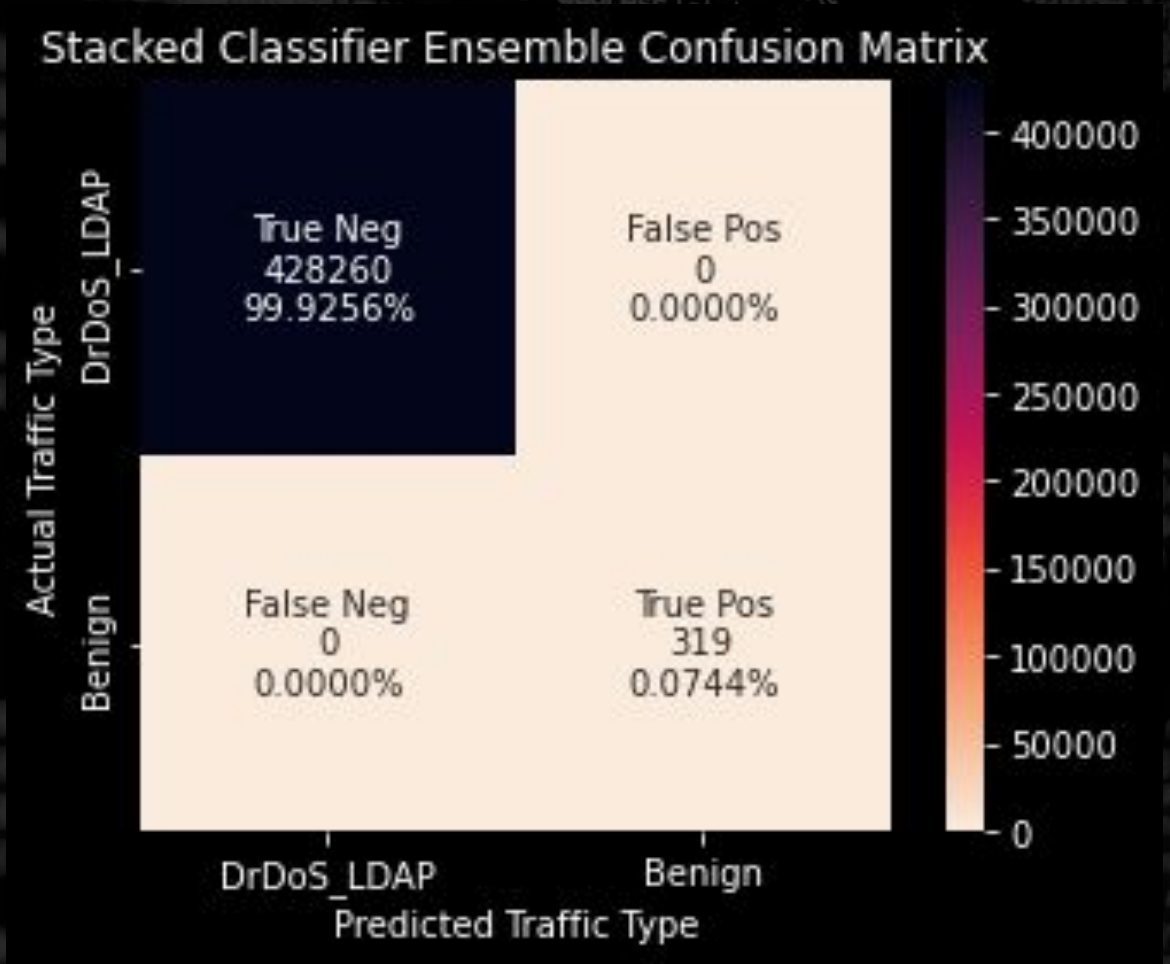


F_2 : .974

Recall: 1

Precision: .883

Stacked Classifier - Validation

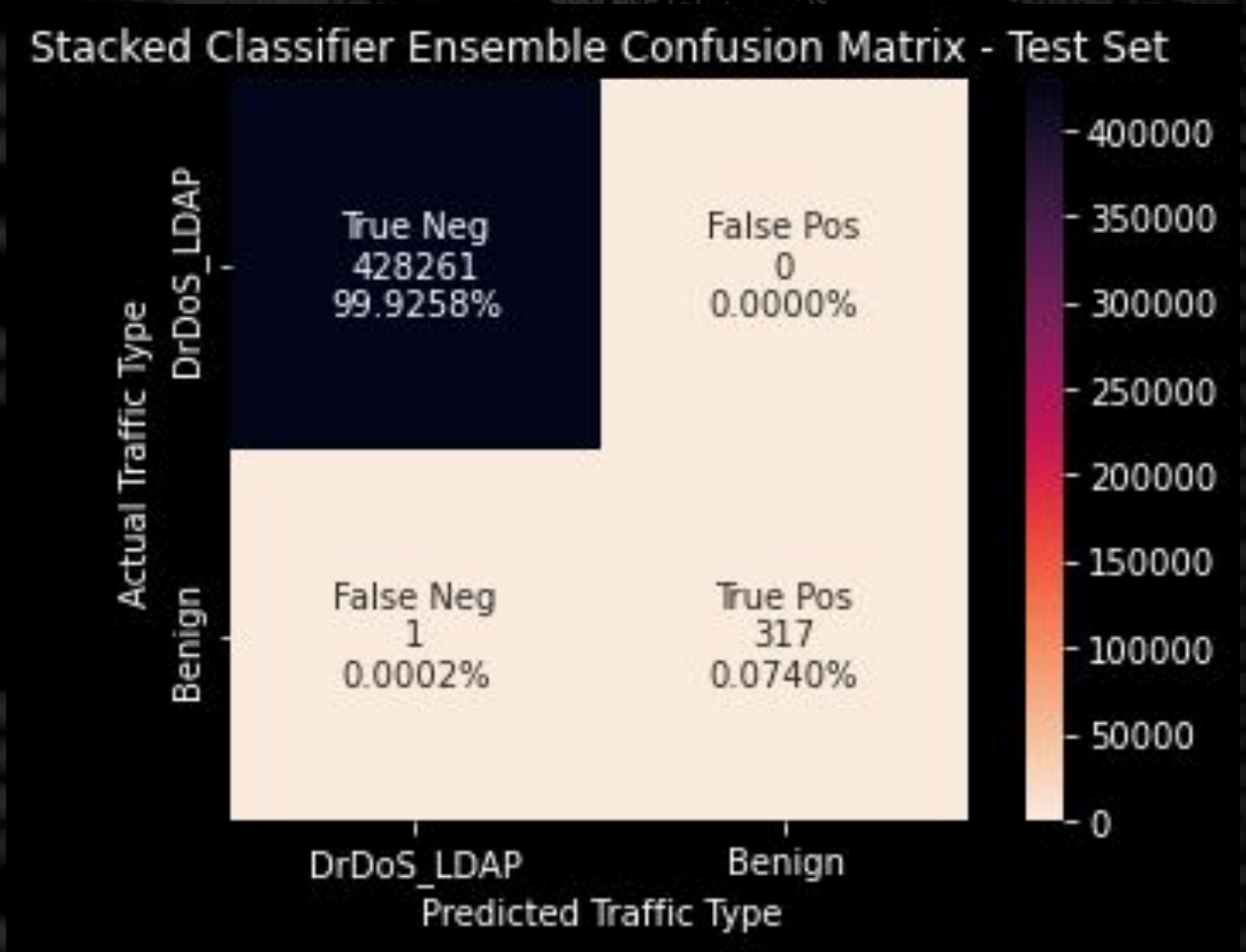


F_2 : 1

Recall: 1

Precision: 1

Stacked Classifier - Final Test Results



F_2 : .997

Recall: .996

Precision: 1

Conclusions

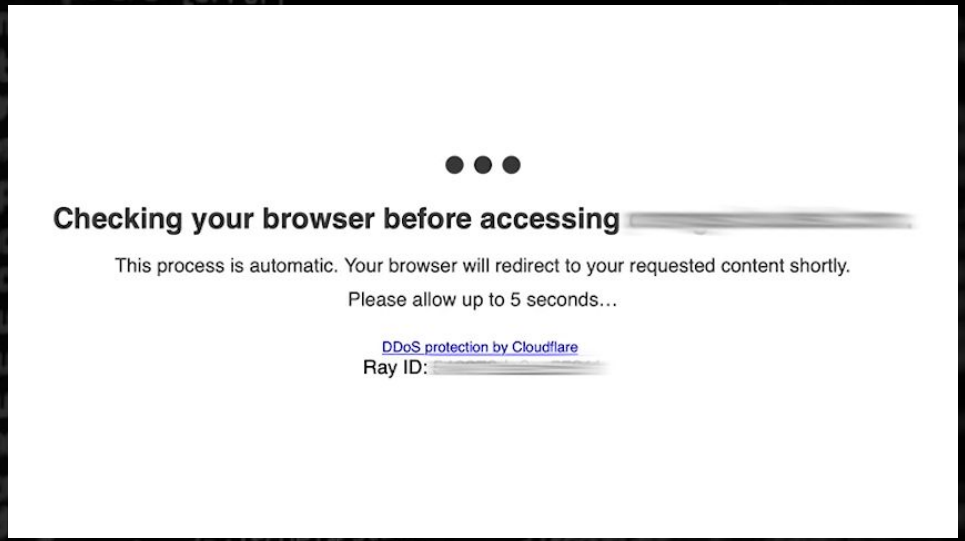
Conclusions

- Viability of using classification to identify malicious/legitimate traffic is proven
- Stacking Classifier Ensemble performs exceptionally well
  - Meets & exceeds business objectives/success metrics
- MinPacketLength traffic feature should be explored further


Validation

Validation

- Additional testing with synthetic attacks
- Deploy model in production
  - Evaluate recall rate on live benign traffic
  - Evaluate precision during DDoS attack
  - Benchmark performance against vendor solutions (e.g. Cloudflare, Akamai)



Further Work

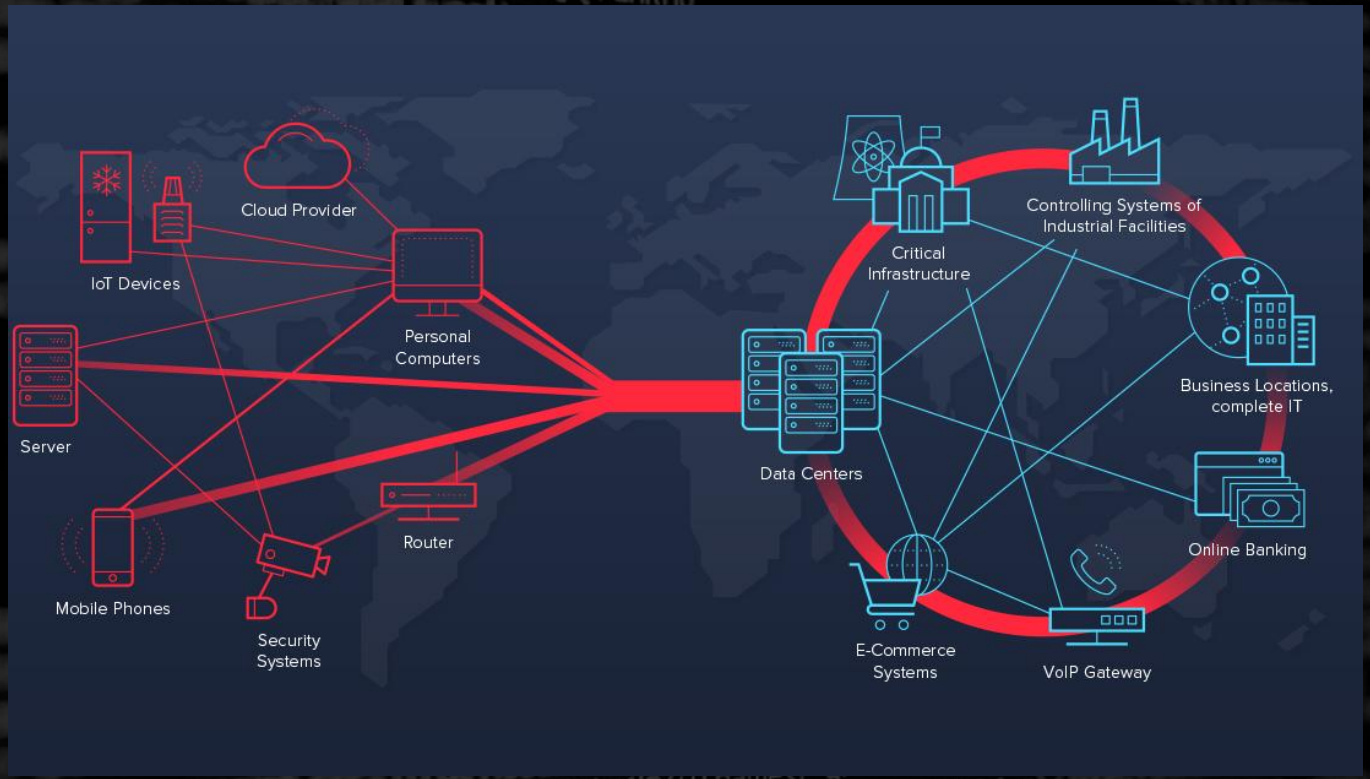
Further Work

- Expand to include more DDoS attack types
- Hyperparameter tuning for models/ensemble
- Reduce model training/prediction time using Dask, RAPIDS cuML
- Additional models in the ensemble (Naive Bayes)

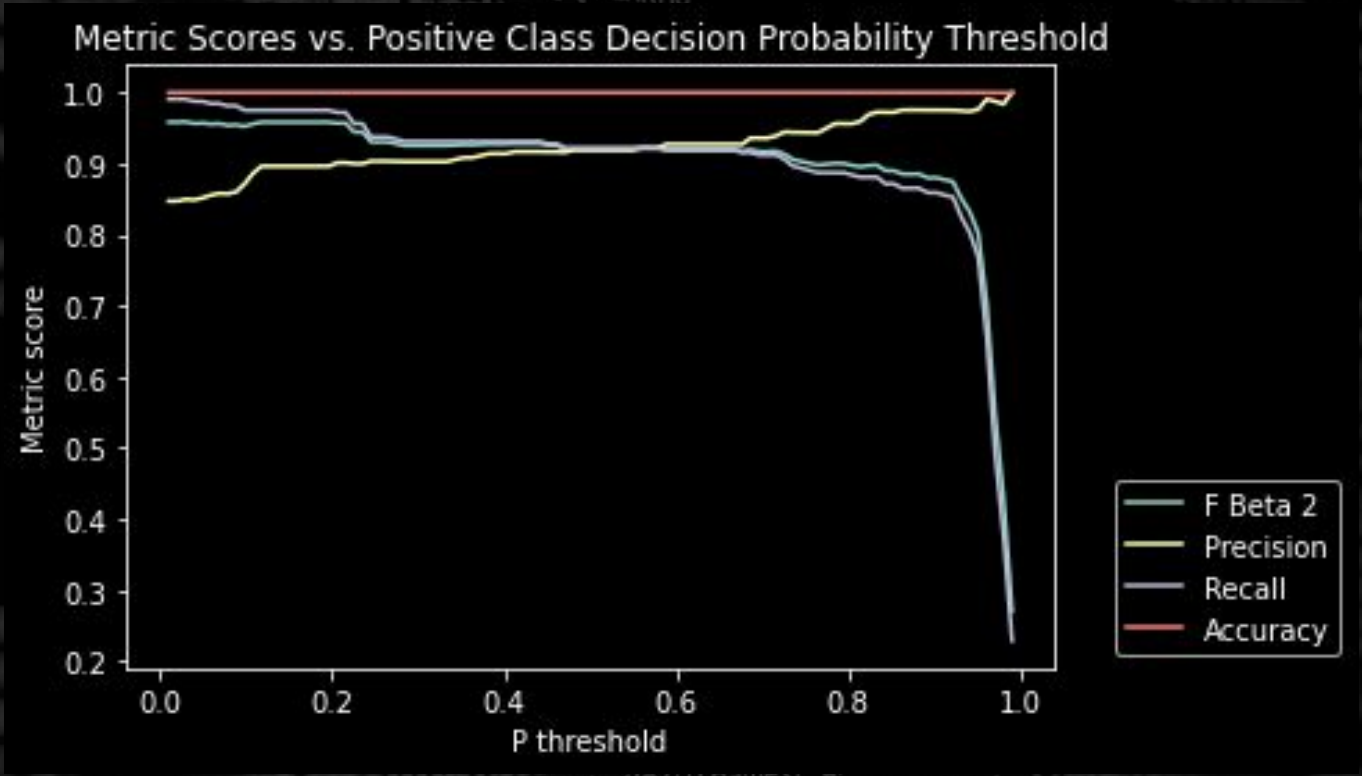

Thank you!

Appendix

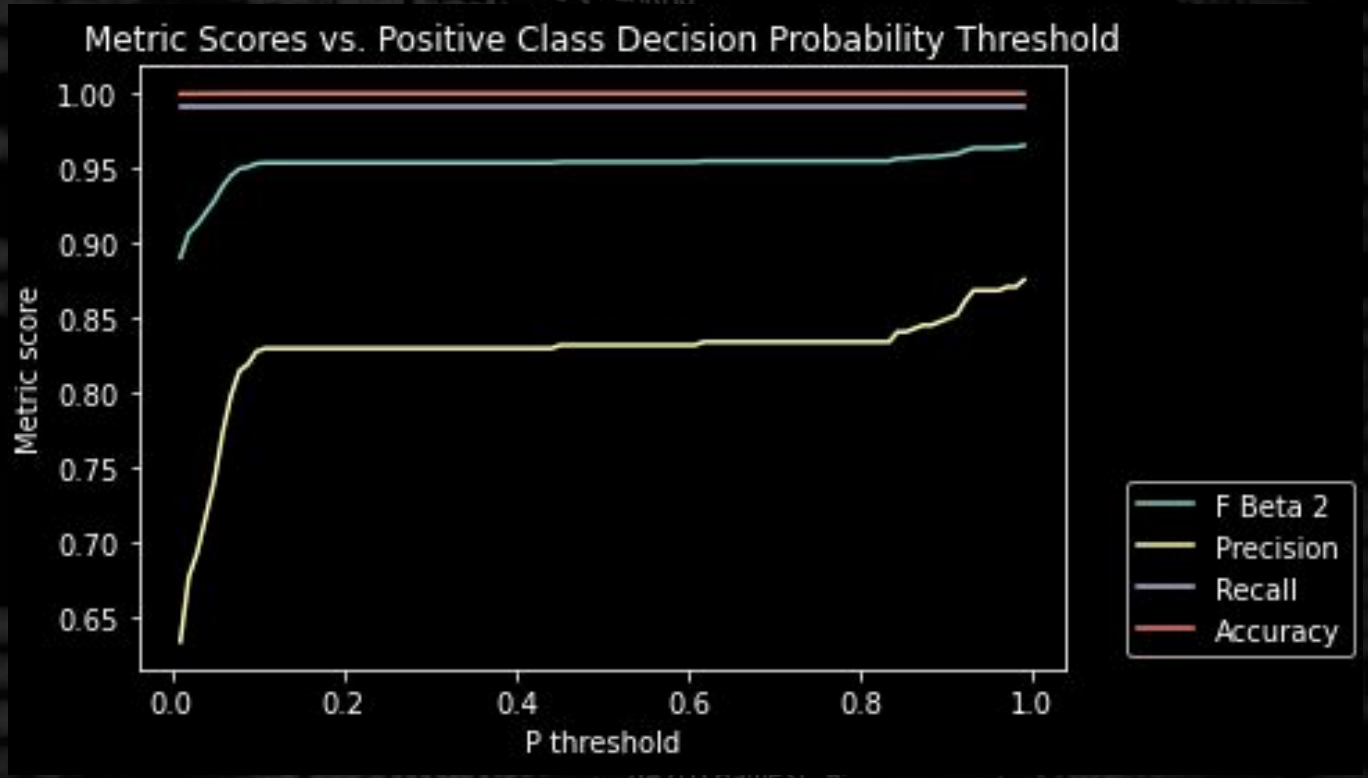
What is a DDoS attack ?



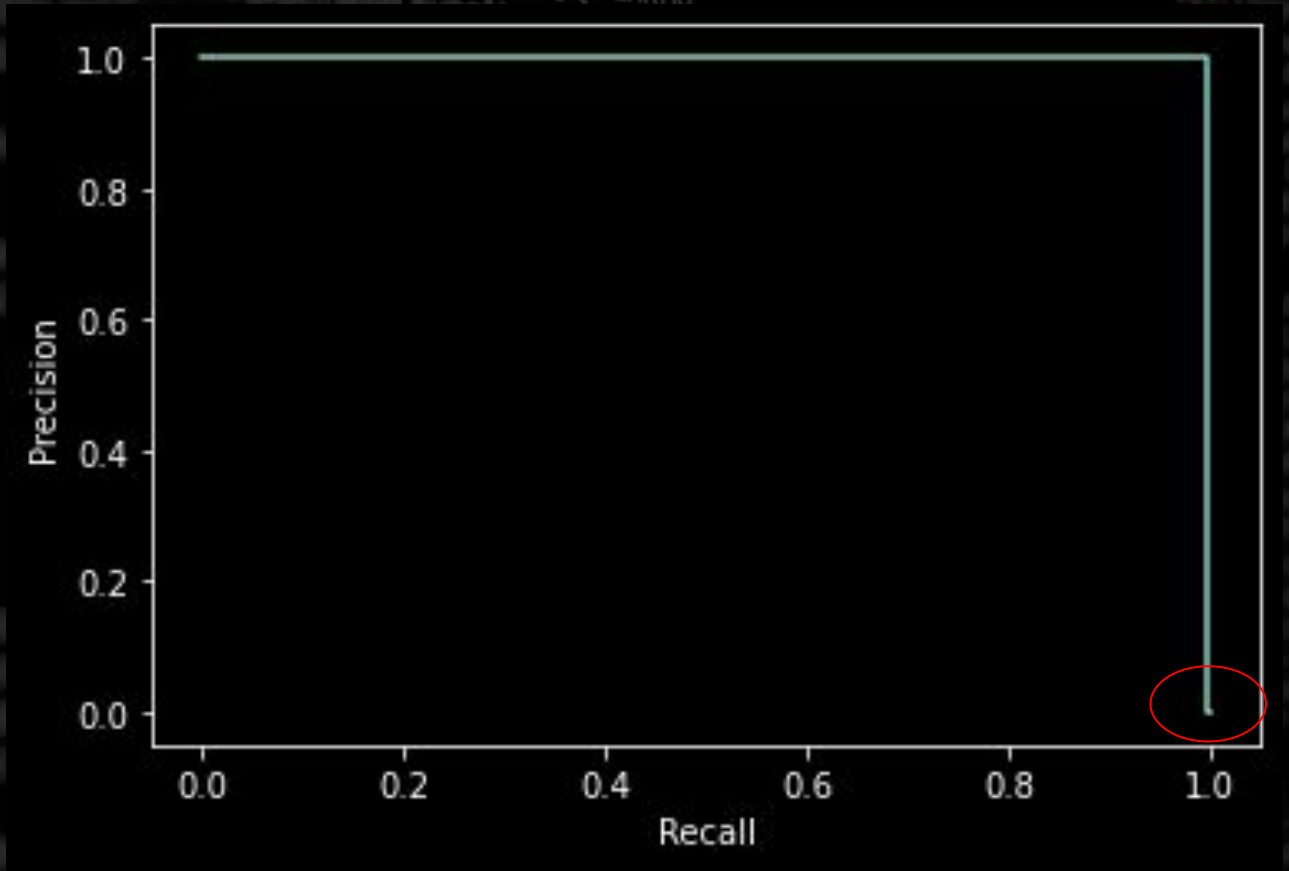
Baseline Logistic Regression Threshold



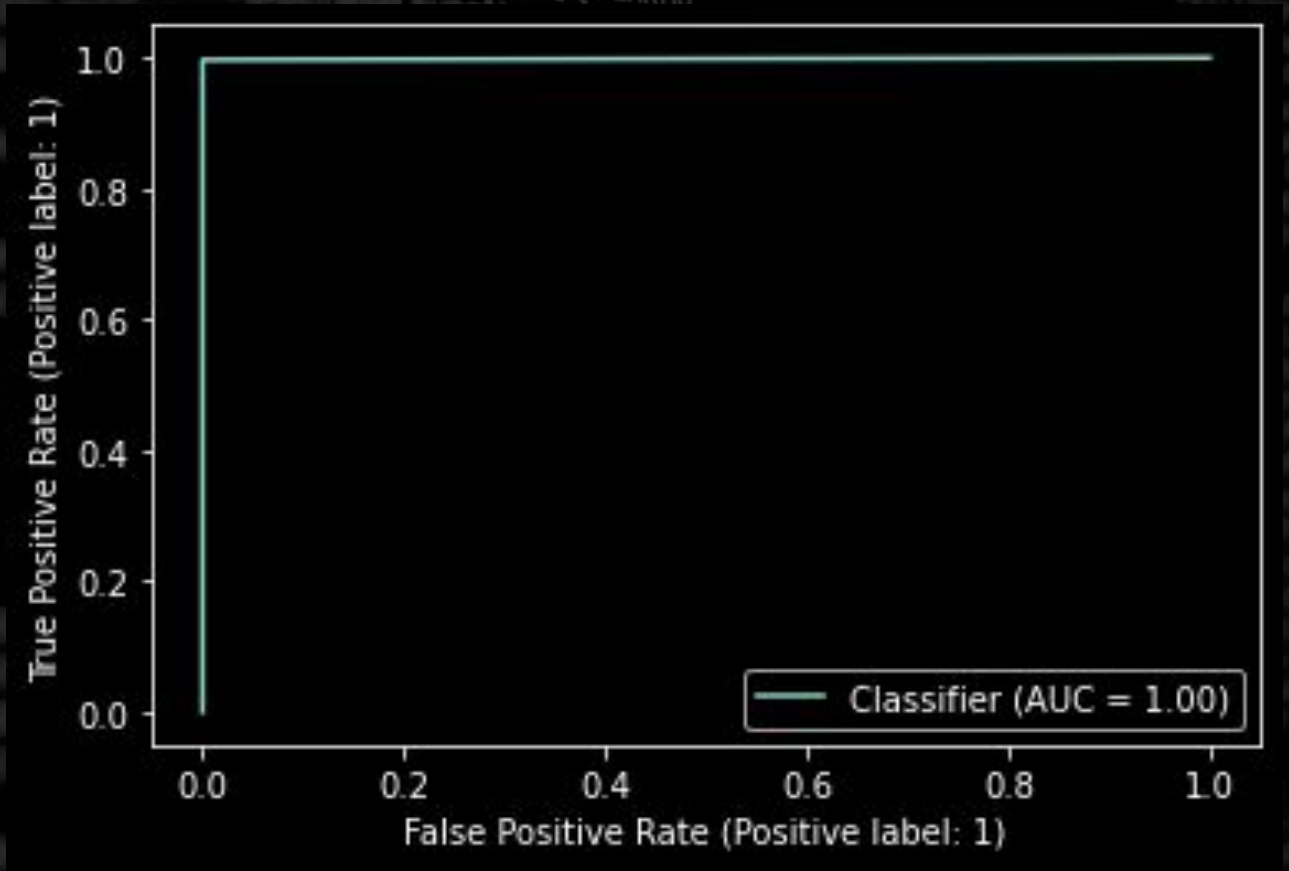
Weighted Logistic Regression Threshold



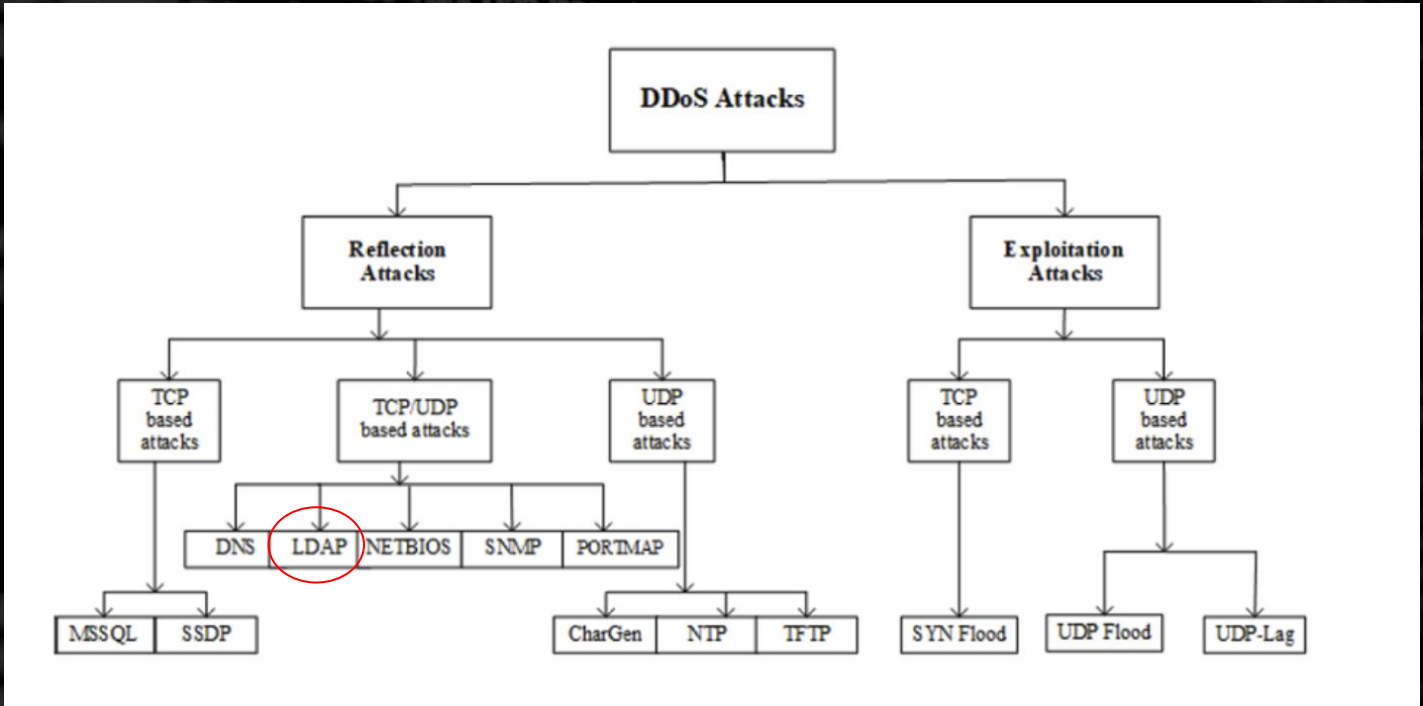
Stacked Classifier Precision/Recall Curve



Stacked Classifier ROC Curve



DDoS Attack Types



Testbed Architecture

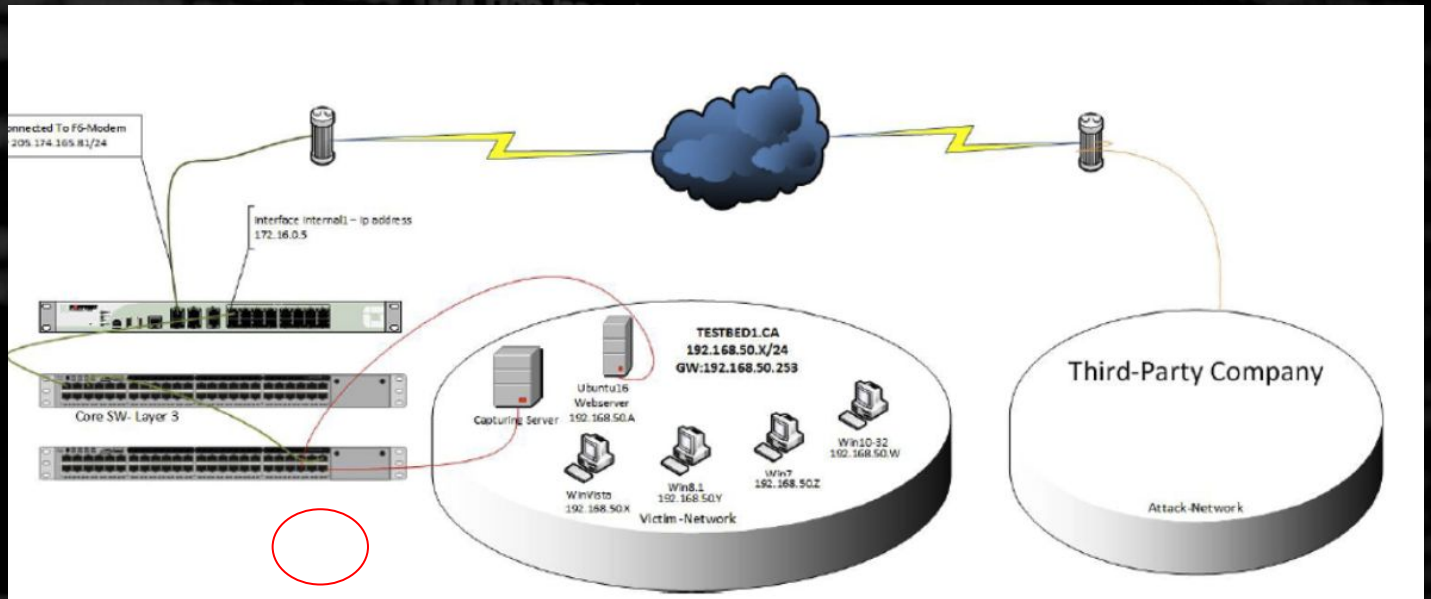


Figure 2: Testbed Architecture