Prevenção de ataques DDOS

Uso de aprendizado de máquina para a prevenção de ataques DDOS

Problema(DDOS)

Uma ataque DDoS tem como objetivo consumir os recursos de um servidor com requisições supérfluas ao ponto de indisponibilizar o seu serviço para usuários verdadeiros.

Ponto importante

Se o agente malicioso não conseguir consumir recursos suficientes do servidor, ele **NÃO** será capaz de alcançar o objetivo do ataque que seria negar o servidor para usuários reais.

Diversos tipos

Existem diversas formas de ataques DDoS, onde cada uma delas tem suas respectivas características. Exemplos:

- UDP flooding
- SYN flooding
- Vulnerabilidade no NetBios

Dataset CIC - DDoS2019

O dataset escolhido foi o CIC - DDoS de 2019, que possui dados gerados artificialmente.

Dados

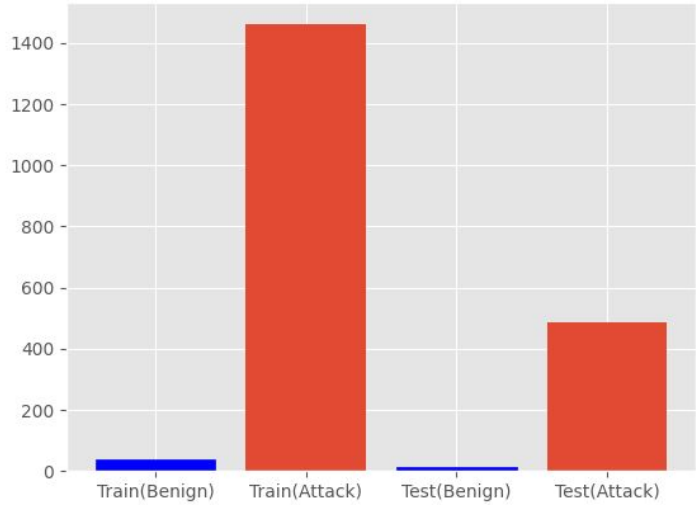
- Dataset contém 88 features
- Nome das features mal formatado
- 6 não são numéricos:
  - Label
  - Flow ID
  - Simillar HTTP
  - Source IP
  - Destination IP
  - Timestamp
- Possui alguns registros vazios
- Dados contendo o resultado de operações matemáticas, como por exemplo desvio padrão, média, variância, etc.

Excesso de dados

O arquivo com menos dados é o Portmap.csv e mesmo assim existe mais de 76.000 linhas de dados. Resampling se tornou necessário.

Distribuição

A distribuição é desbalanceada, com em torno de 90% de dados de ataque e apenas ~10% de dados benignos.



Objetivo da solução

A solução proposta deve cumprir com os seguintes objetivos:

- Deve bloquear requisições maliciosas o suficiente para impedir o uso excessivo dos recursos providos pelo servidor
- Conter o mínimo possível de casos falsos-positivos

Estimadores

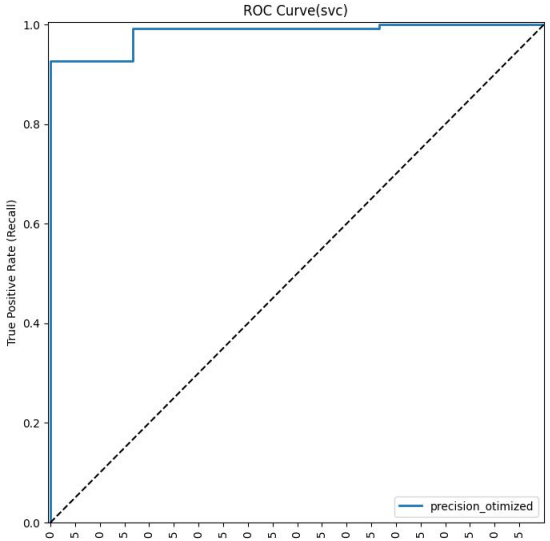
Os estimadores utilizados foram:

- Random Forest
- KNN
- SVM

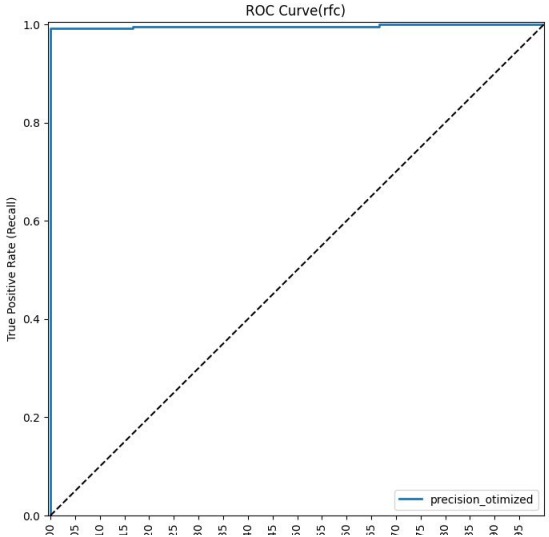
Hiperparâmetros

Para a otimização dos hiperparâmetros dos estimadores foi utilizado o Grid Search com o foco na métrica de **precisão**.

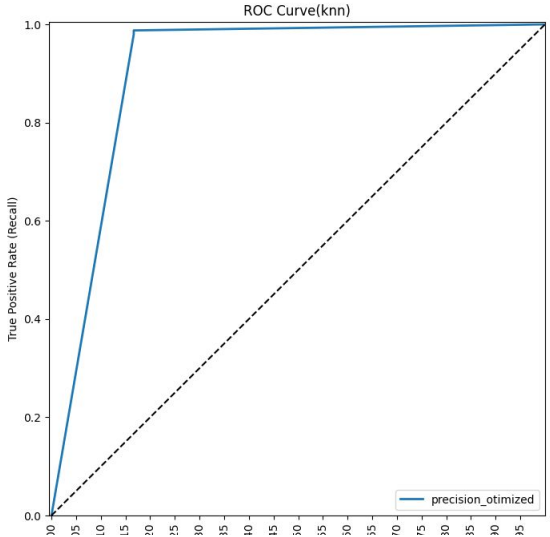
Resultados



0.983



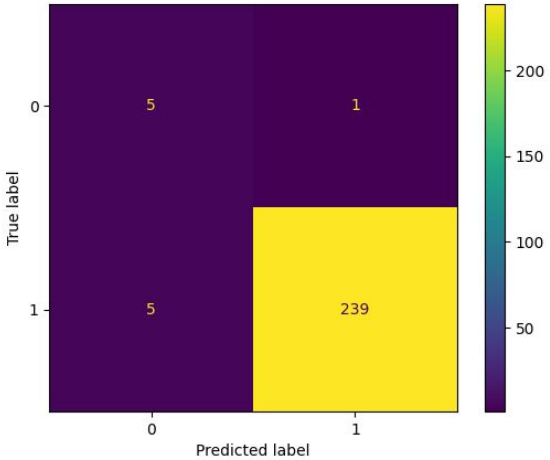
0.996



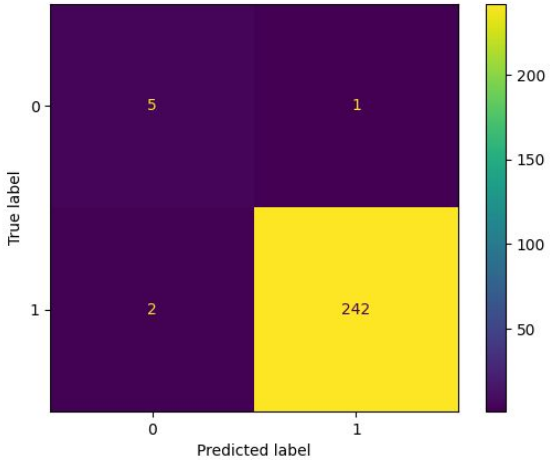
0.909

Resultados

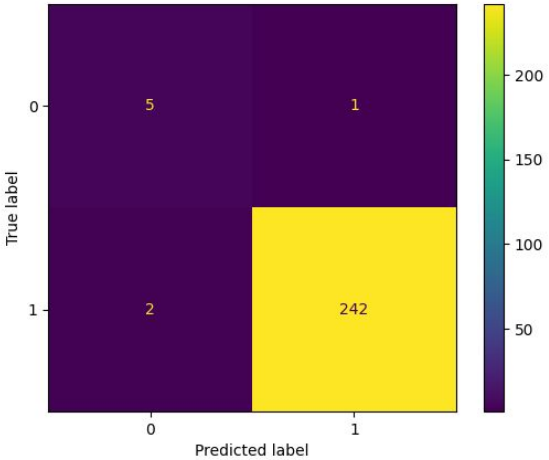
KNN



Random Forest



SVC



Preocupações

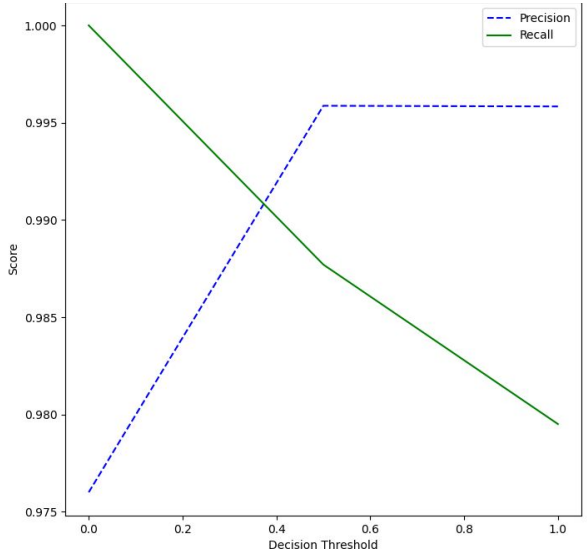
É comum a Random Forest gerar um *overfitting* e como ela teve um resultado tão excelente, gerou suspeitas.

Mitigar o problema do Falso-Positivo

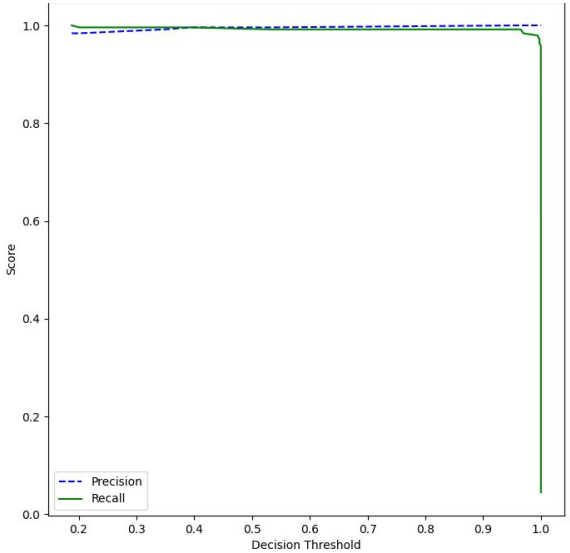
Foi utilizado um limiar sobre a probabilidade de um dado pertencer a uma classe para garantir que ele seja considerado um ataque somente se o modelo tem um certo grau de certeza.

Resultados

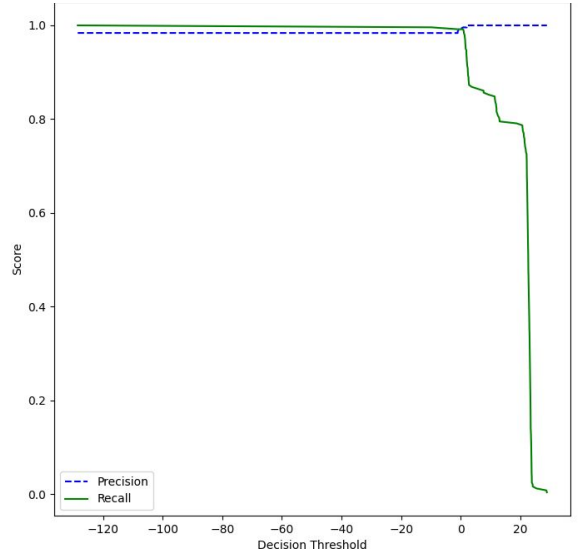
KNN



Random Forest



SVC



Outras possíveis soluções

Por causa do fato de que os casos de falso-positivo foram tão baixo, outras soluções não foram implementadas.

Referências

https://www.unb.ca/cic/datasets/ddos-2019.html

https://scikit-learn.org/stable/user_guide.html

https://pandas.pydata.org/docs/