DETECÇÃO DE ATAQUES EM FLUXOS DE REDE UTILIZANDO NAIVE BAYES

Carolina Gabriela, Eduardo Alves, Isabela Moura,
Karina Lima, Kauanny Barros

CIC-IDS2017

Nosso dataset é amplamente utilizado para IDS e IPS

Possui tráfego de rede benigno e ataques comuns

Dados capturados por meio de pacotes de rede (PCAPs)

Possui dados capturados entre 3 e 7 de julho de 2017

Inclui ataques como DoS, DDos, Web Attack, Brute Force FTP/SSH

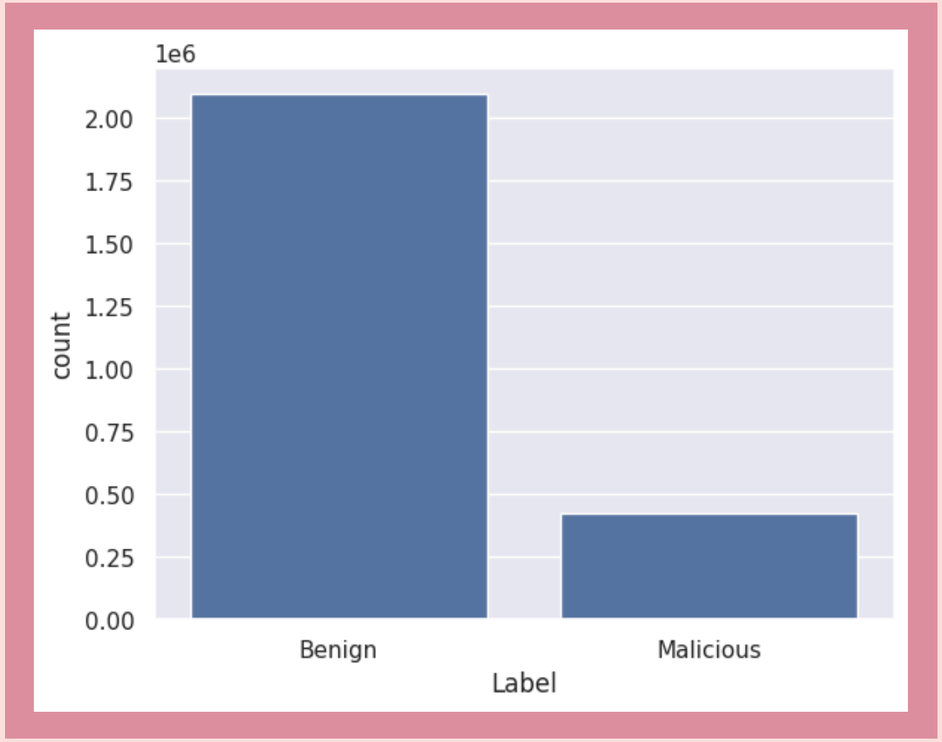
Possui informações como IPs, portas, protocolos e tipos de ataques

PROCESSAMENTO DO DATASET

- Padronização e Limpeza dos dados
  - Remoção de espaços, registros duplicados e valores ausentes
- Separação dos dados em treino e teste
- Análise de correlação das features para eliminar redundâncias
- Normalização das variáveis para garantir comparabilidade

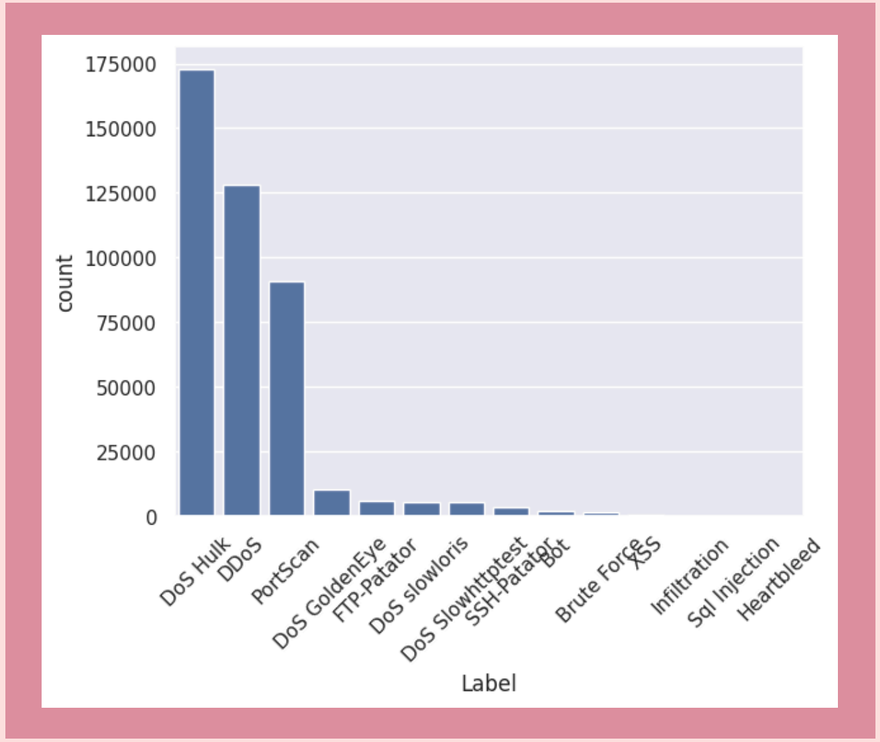
ANÁLISE EXPLORATÓRIA DOS DADOS

- Predominância de tráfego benigno
  - Desbalanceamento entre classes devido a maior ocorrência de tráfego legítimo



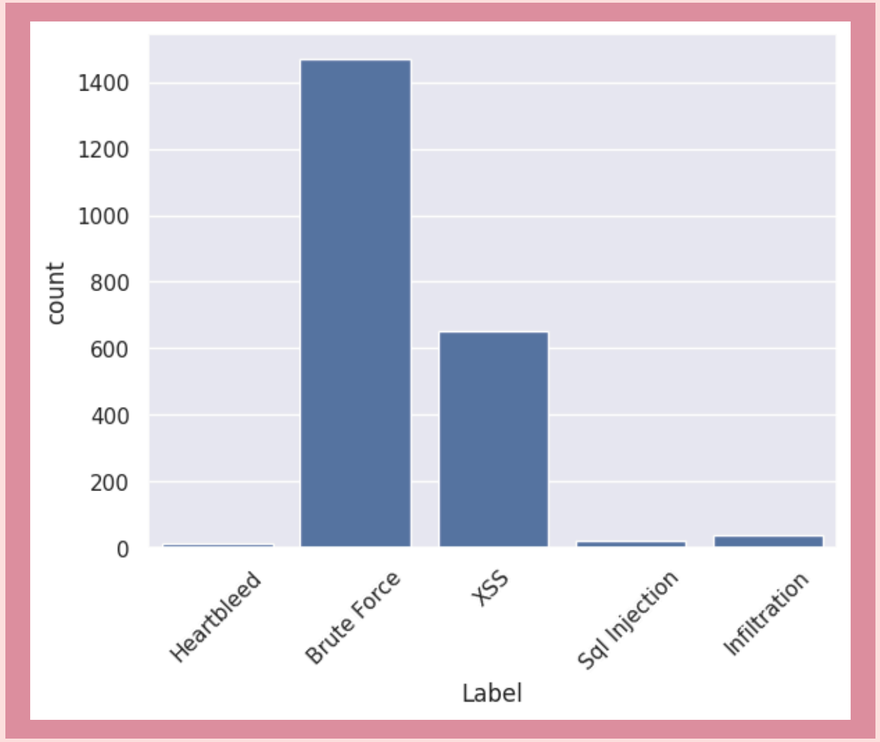
ANÁLISE EXPLORATÓRIA DOS DADOS

- Ataques mais frequentes DoS Hulk e DDoS
  - Que geram um alto volume de requisições



ANÁLISE EXPLORATÓRIA DOS DADOS

- Os ataques Heartbleed, SQL Injection e Infiltration apresentam uma ocorrência significativamente menor em comparação com os demais



ANÁLISE EXPLORATÓRIA DOS DADOS

	Destination Port	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total Length of Bwd Packets	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std	...
count	2.522009e+06	2.522009e+06	2.522009e+06	2.522009e+06	2.522009e+06	2.522009e+06	2.522009e+06	2.522009e+06	2.522009e+06	2.522009e+06	...
mean	8.701432e+03	1.658364e+07	1.027750e+01	1.156751e+01	6.116607e+02	1.813569e+04	2.311241e+02	1.919733e+01	6.347899e+01	7.728840e+01	...
std	1.902225e+04	3.522618e+07	7.942294e+02	1.056668e+03	1.058573e+04	2.397602e+06	7.562104e+02	6.079830e+01	1.955137e+02	2.968147e+02	...
min	0.000000e+00	-1.300000e+01	1.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	...
25%	5.300000e+01	2.080000e+02	2.000000e+00	1.000000e+00	1.200000e+01	6.000000e+00	6.000000e+00	0.000000e+00	6.000000e+00	0.000000e+00	...
50%	8.000000e+01	5.058700e+04	2.000000e+00	2.000000e+00	6.600000e+01	1.560000e+02	4.000000e+01	2.000000e+00	3.613084e+01	0.000000e+00	...
75%	4.430000e+02	5.330376e+06	6.000000e+00	5.000000e+00	3.320000e+02	9.910000e+02	2.020000e+02	3.700000e+01	5.200000e+01	7.417179e+01	...
max	6.553500e+04	1.200000e+08	2.197590e+05	2.919220e+05	1.290000e+07	6.554530e+08	2.482000e+04	2.325000e+03	5.940857e+03	7.125597e+03	...

8 rows × 78 columns

- Utilizando o comando *dataset.describe()* recebemos algumas medidas interessantes que foram a contagem dos valores, a média, a mediana, o desvio padrão, os valores de mínimo e máximo, os quartis 25% e 75% de cada coluna do dataset

Teorema de Bayes

- Utilizado para calcular a probabilidade de um evento com base em informações prévias relacionadas a ele
- Descreve como ajustar uma estimativa inicial ao considerar novas evidências ou dados observados, produzindo uma probabilidade revisada mais precisa

$$P(A|B) = \frac{P(B|A) \times P(A)}{P(B)}$$

- Baseado no Teorema de Bayes
- Assume independência condicional entre os atributos
- Simples, eficiente e adequado para grandes volumes de dados
- Apresenta uma abordagem direta e eficiente para resolver problemas de classificação, com base em princípios estatísticos sólidos.

CLASSIFICADOR INGÊNUO DE BAYES

VARIAÇÕES EXPERIMENTADAS

- Gaussian Naive Bayes
  - Assume que os atributos seguem uma distribuição normal dentro de cada classe
  - Indicado para dados contínuos
- Bernoulli Naive Bayes
  - Usa a distribuição de Bernoulli (0 ou 1)
  - Ideal para dados binários
  - Robusto para dados esparsos

FERRAMENTAS UTILIZADAS

seaborn

pandas

Mais algumas bibliotecas:

- Os
- Re
- Google

NumPy

matplotlib

scikit learn

MÉTRICAS UTILIZADAS

- **Acurácia**: Proporção de previsões corretas
- **True Positive Rate (TPR)**: Taxa de verdadeiros positivos
- **TPR por ataque**: Desempenho na identificação de cada ataque
- **False Positive Rate (FPR)**: Taxa de falsos positivos
- **Precisão**: Proporção de verdadeiros positivos entre todas as previsões positivas
- **Recall**: Capacidade de identificar corretamente uma classe
- **F1-score**: Média harmônica entre precisão e recall
- **Matriz de Confusão**: Representação visual dos erros e acertos
- **Curva ROC** e **AUC-ROC**: Avaliação da relação TPR x FPR

ANÁLISE DOS RESULTADOS

Gaussian Naive Bayes (GaussianNB)

- Algoritmo mais usado com variáveis contínuas que seguem uma distribuição gaussiana.

Bernoulli Naive Bayes (BernoulliNB)

- Algoritmo mais adequado para variáveis binárias.
- Boa performance com valores booleanos.

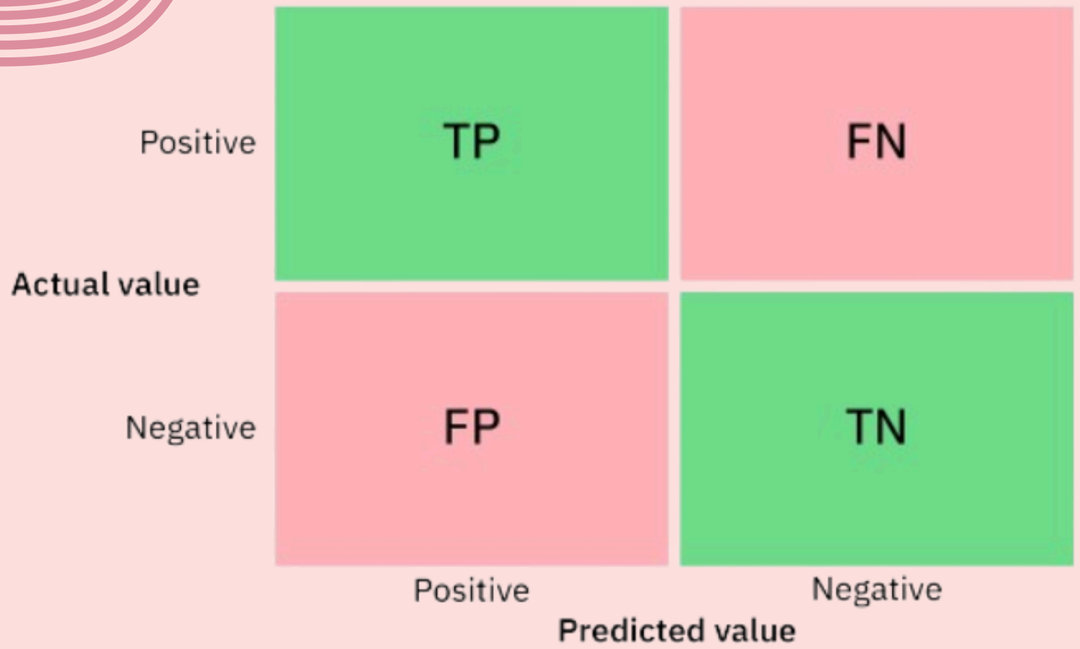
GAUSSIAN NAIVE BAYES

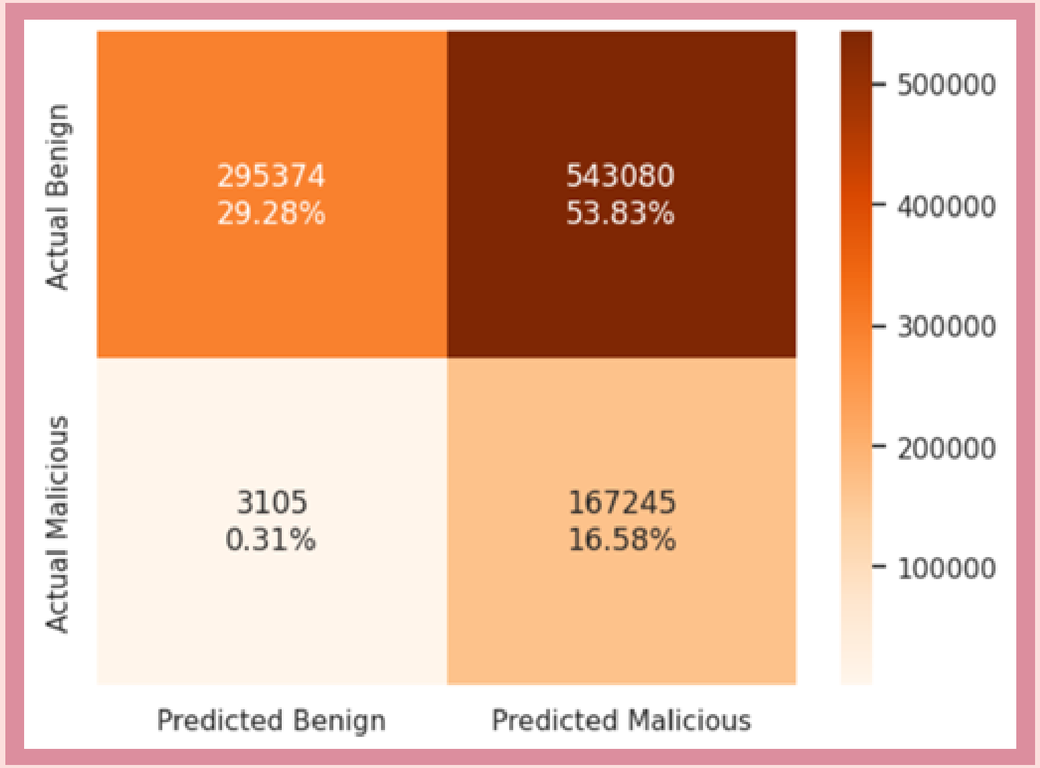
Classification Report:

	precision	recall	f1-score	support
0	0.99	0.35	0.52	838454
1	0.24	0.98	0.38	170350
accuracy			0.46	1008804
macro avg	0.61	0.67	0.45	1008804
weighted avg	0.86	0.46	0.50	1008804

- Alta sensibilidade (recall) na detecção de ataques.
- Baixa precisão na detecção de ataques.
- Baixo recall na classe de tráfego benigno.

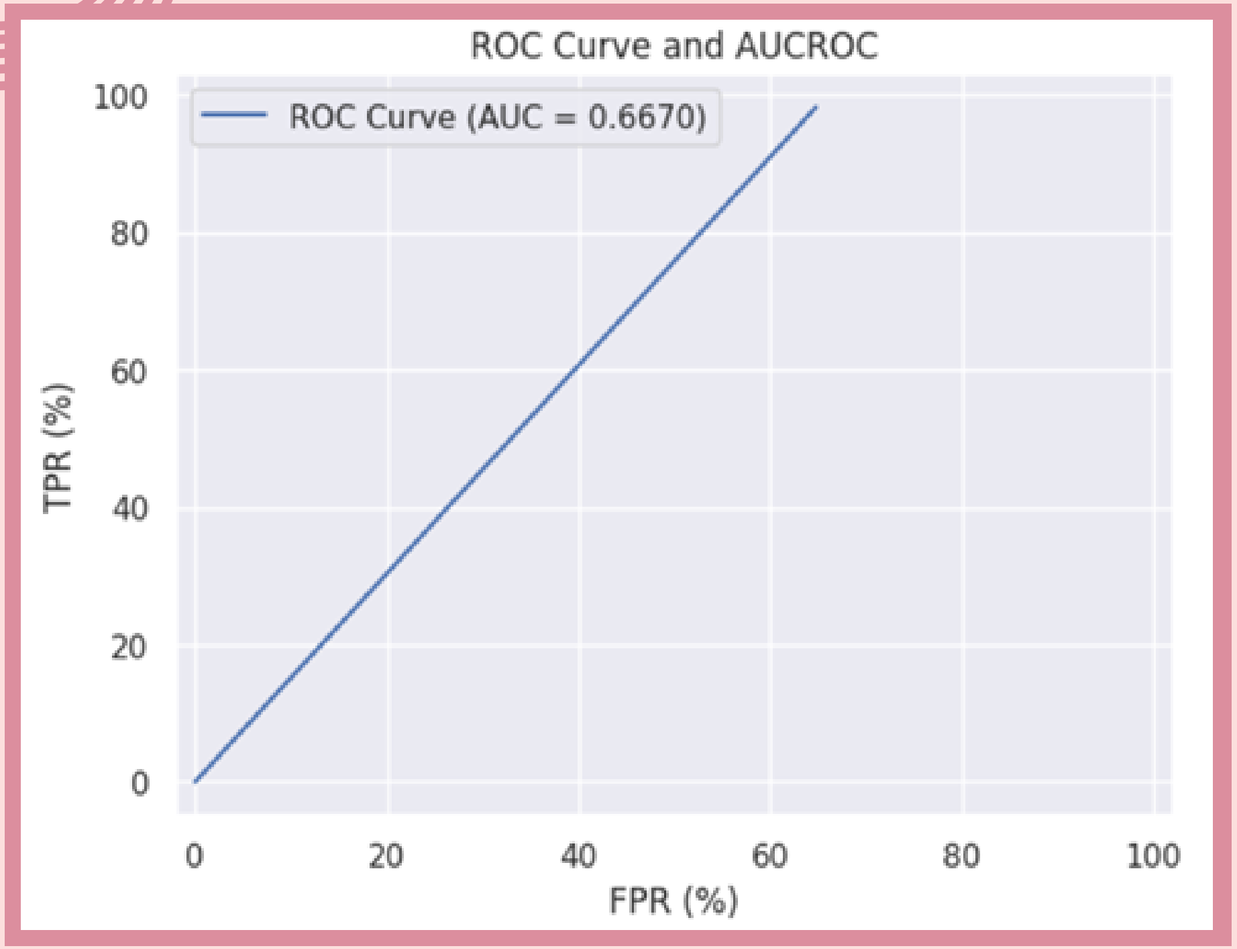
Matriz de confusão





- Grande quantidade de falsos negativos.
- Pequena quantidade de falsos positivos.

ROC Curve



AUC = 1: modelo perfeito
AUC = 0.5: desempenho de um classificador aleatório

- Curva que sobe rápido no eixo Y (Taxa de Verdadeiros Positivos).
- Taxa de Falsos Positivos cresce rápido também.

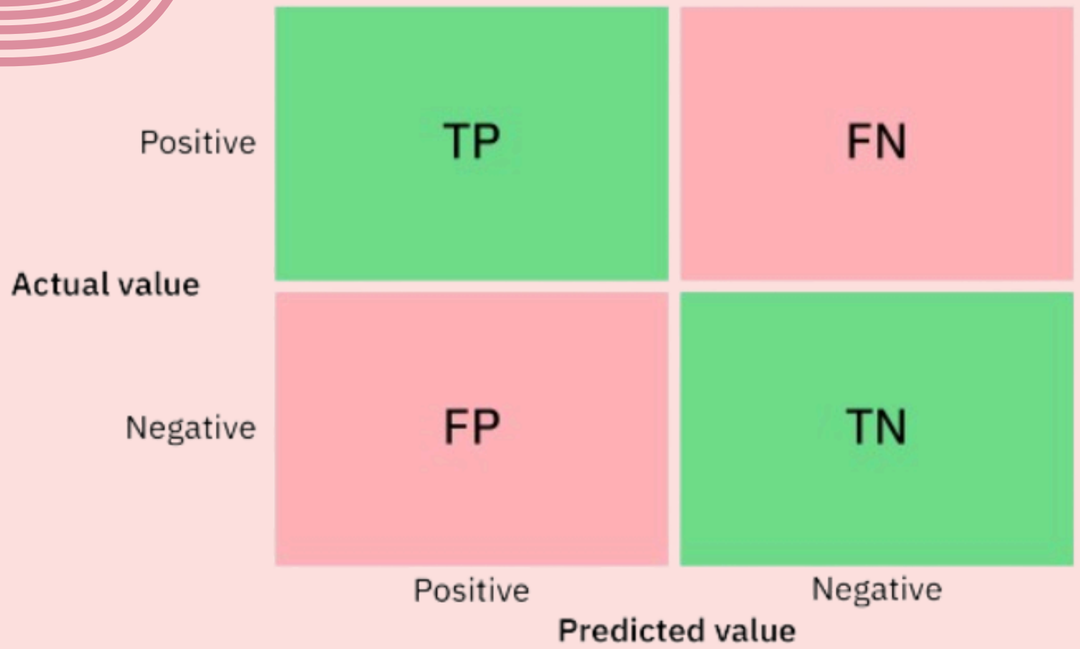
BERNOULLI NAIVE BAYES

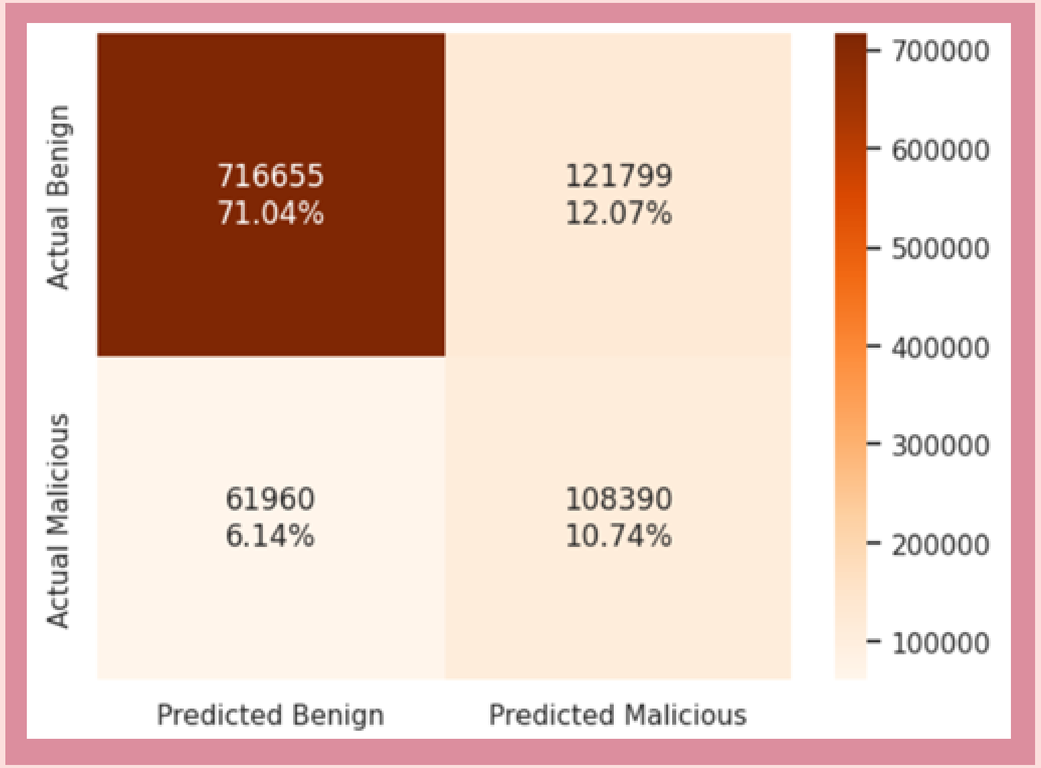
Classification Report:

	precision	recall	f1-score	support
0	0.92	0.85	0.89	838454
1	0.47	0.64	0.54	170350
accuracy			0.82	1008804
macro avg	0.70	0.75	0.71	1008804
weighted avg	0.84	0.82	0.83	1008804

- Equilíbrio superior entre precisão e recall nas duas classes.
- Alta sensibilidade e precisão para tráfego normal.
- Mais eficaz do que o GaussianNB para esse dataset.

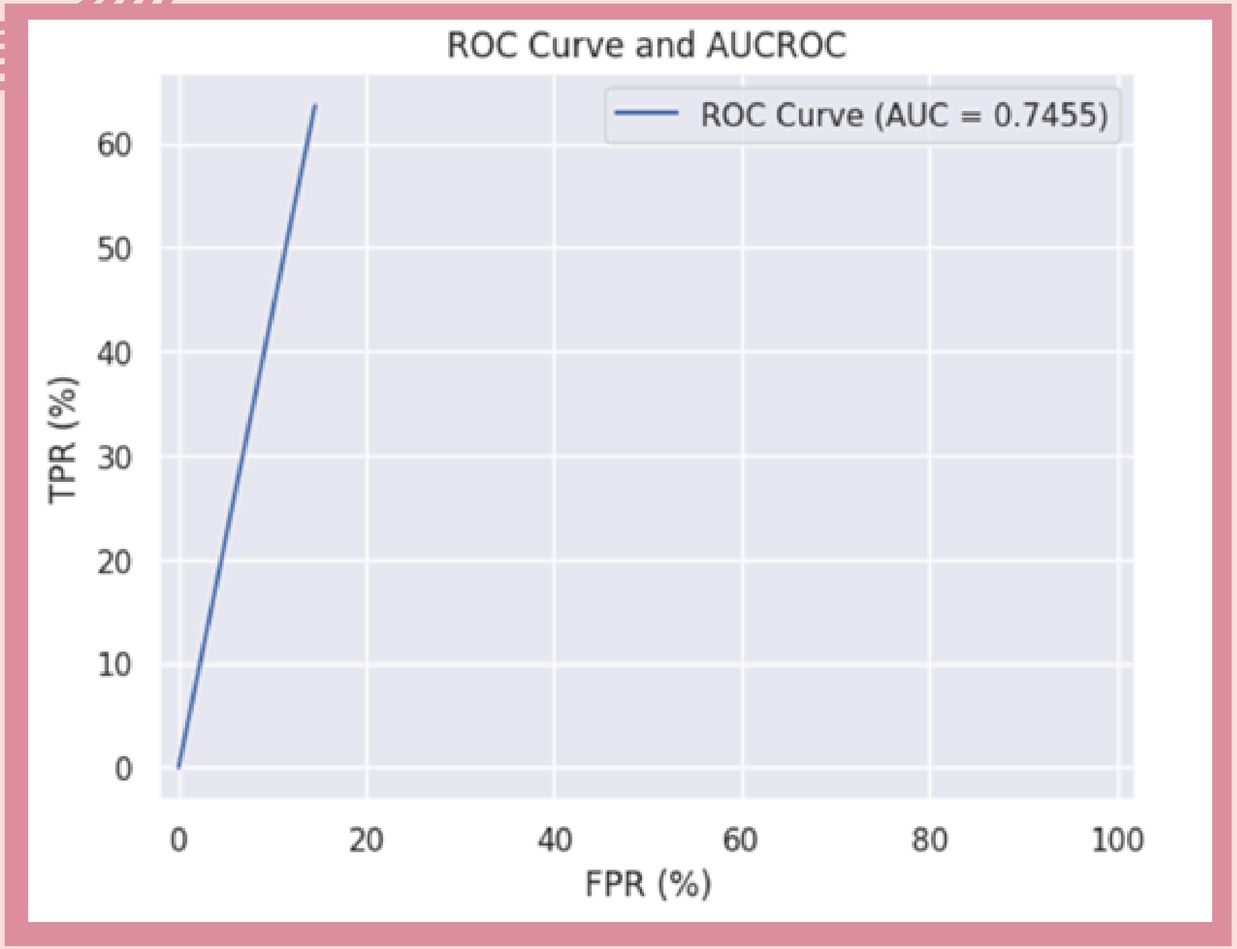
Matriz de confusão





- Pequena quantidade de falsos negativos.
- Apresenta maior quantidade de falsos positivos.

ROC Curve



AUC = 1: modelo perfeito
AUC = 0.5: desempenho de um classificador aleatório

- Curva melhor balanceada.
- Modelo consegue diferenciar melhor o que é ataque e o que é benigno.

CONCLUSÃO

- GaussianNB detecta a maior parte dos ataques, mas com um alto índice de falsos negativos.
- BernoulliNB demonstrou melhor equilíbrio entre precisão e recall.

- Possibilidades de melhorias futuras:
  - Aprimoramento no tratamento de dados;
  - Testes de outros algoritmos de Machine Learning;
  - Busca por modelos mais eficazes na detecção de ataques.

OBRIGADO PELA ATENÇÃO!