

Comparação de Modelos Classificadores na Detecção de Anomalias em Sistemas de Detecção de Intrusão

> ◎ ≈

Sumário

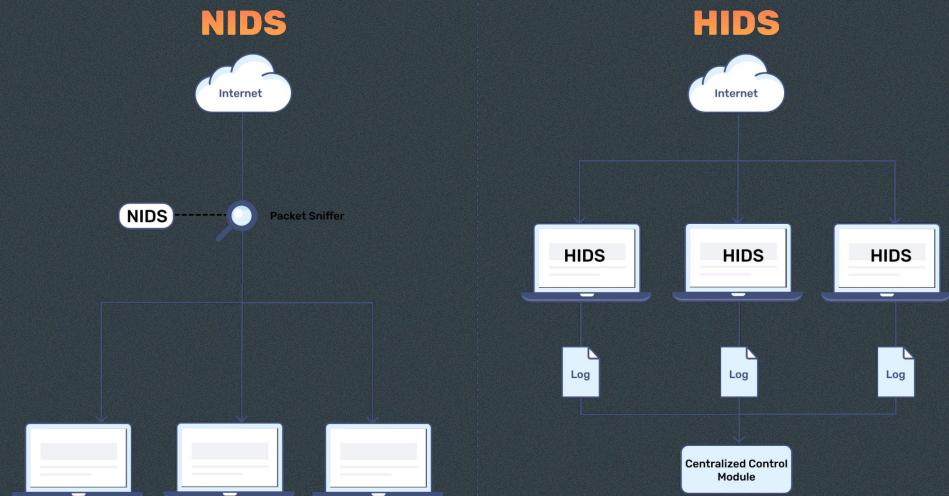
— □ ×

1. Introdução
2. Motivação e Objetivo
3. Metodologia
4. Resultados
5. Conclusão

Introdução

— □ ×

- O que é um Sistema de Detecção de Intrusão?
- Tipos: host e redes sem fio
- Identificam ataques por assinatura ou por anomalia



Motivação e Objetivo

— □ ×

- Por que é interessante?
- Expansão da digitalização
- Aumento das ameaças

- Comparação de modelos de aprendizagem de máquina.
- Encontrar o mais adequado.

Metodologia

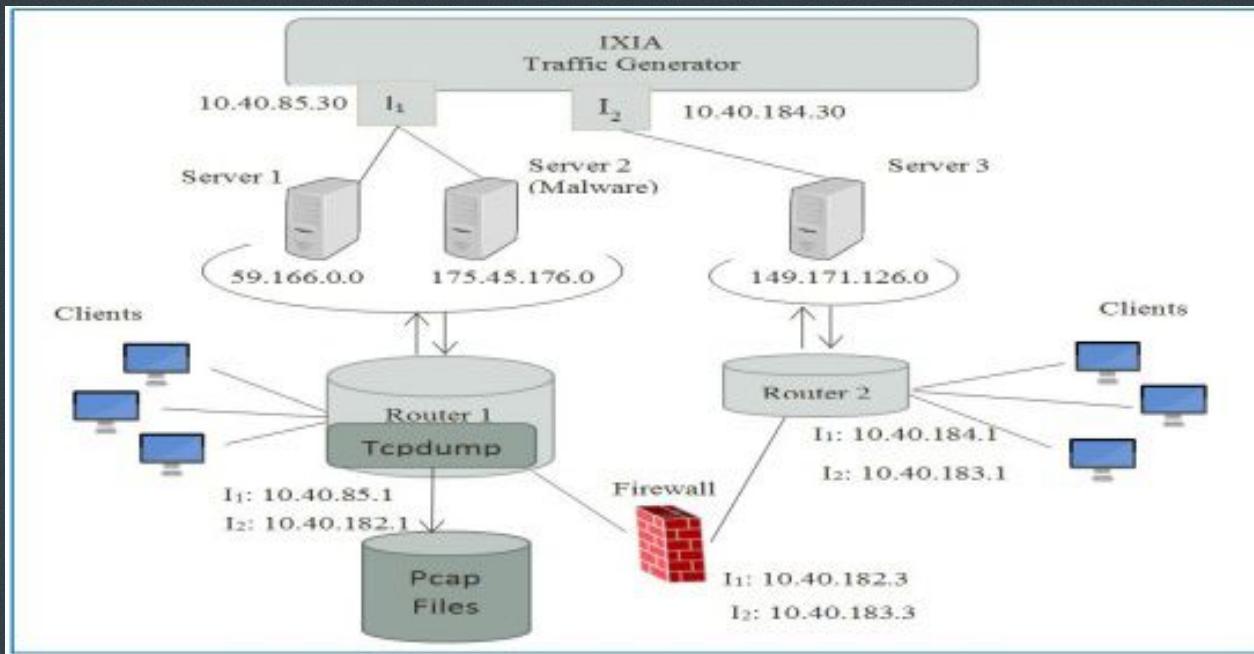
— □ ×

- Ferramentas: Jupyter, Pandas, Numpy, Scikit-Learn e Hiclass
- Base de dados: UNSW-NB15
 - 2.5M de exemplos
 - 47 Características



Metodología

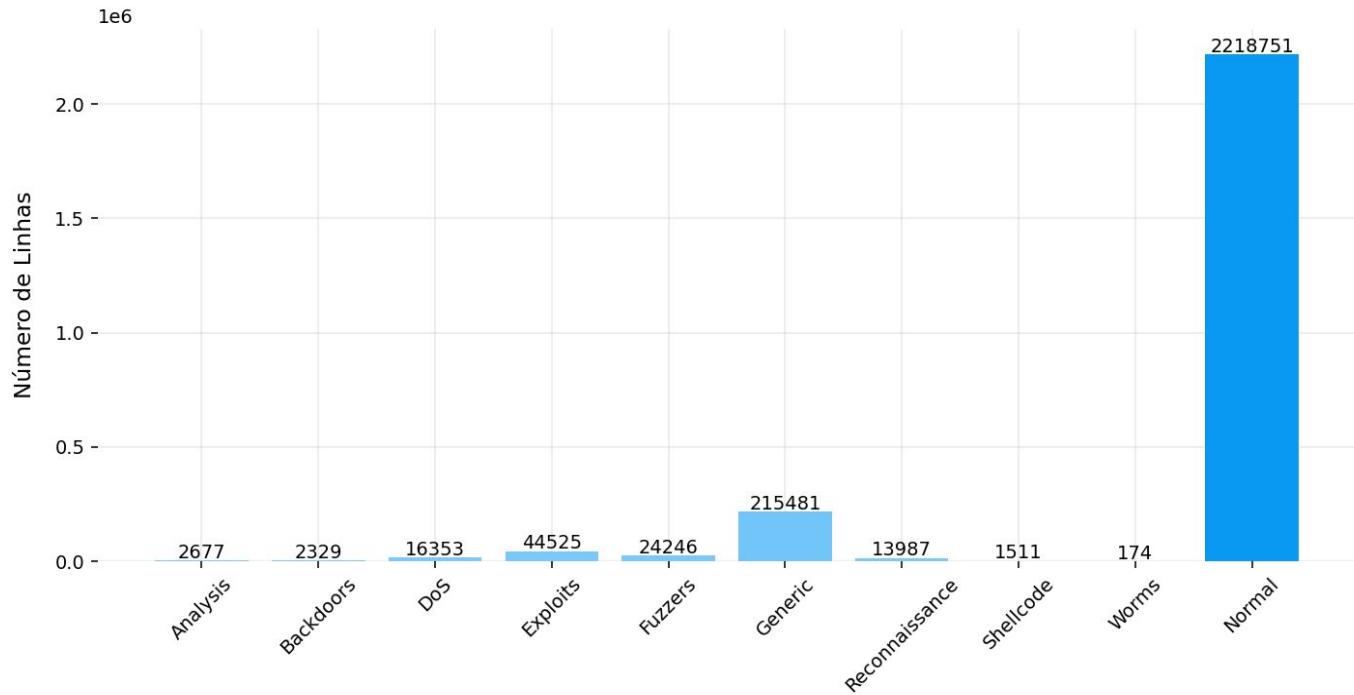
— □ ×



Metodologia

Base de Dados UNSW-NB15

Quantidade de exemplos das classes da base



Pré-processamento dos dados

- União do conjunto
- Busca por inconsistências:
 - Dados faltantes
 - Inconsistências de tipos e formatos
- Normalização

Seleção de Características

— □ ×

- GridSearchCV no Random Forest
- Treino do modelo em Cross Val
- Média das importâncias das características

Feature	Random Forest Feature Importance
dstip	0.171892
sttl	0.171047
ct_state_ttl	0.158517
sbytes	0.085213
srcip	0.080752
dmeansz	0.031187
smeansz	0.030895
dbytes	0.025733

Execução dos Modelos

— □ ×

- Modelos executados:
 - Adaptive Boosting
 - Random Forest
 - XGBoost
 - Bagging
 - MLP
 - Classificador Local por Nível,
por Nível Pai e por Nível.
- Validação cruzada
- Métricas coletadas:
 - acurácia, precisão, recall, f1-score

Resultados

— □ ×

Bagging

	Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1
Normal	0.986528	0.991463	0.999716	0.984851	0.992228
Attack	0.986528	0.991463	0.905347	0.998075	0.949452

Adaptive Boosting

	Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1
Normal	0.99008	0.984432	0.996627	0.991997	0.994306
Attack	0.99008	0.984432	0.946629	0.976867	0.961496

MLP

	Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1
Normal	0.989932	0.981786	0.995765	0.992697	0.994227
Attack	0.989932	0.981786	0.950908	0.970876	0.960703

Resultados

— □ ×

Random Forest

	Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1
Normal	0.992835	0.981564	0.995139	0.996663	0.995900
Attack	0.992835	0.981564	0.976767	0.966465	0.971588

Extreme Gradient Boosting

	Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1
Normal	0.992021	0.982725	0.995682	0.995178	0.995430
Attack	0.992021	0.982725	0.966901	0.970272	0.968583

	Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1		Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1		
Analysis	0.873237		0.1	NaN	0.0	0.000000	Analysis	0.963769		0.42039	0.049700	0.460048	0.089426
Backdoors	0.873237		0.1	NaN	0.0	0.000000	Backdoors	0.963769		0.42039	0.033755	0.036515	0.025713
DoS	0.873237		0.1	NaN	0.0	0.000000	DoS	0.963769		0.42039	0.247432	0.138318	0.135973
Exploits	0.873237		0.1	NaN	0.0	0.000000	Exploits	0.963769		0.42039	0.643191	0.561701	0.585021
Fuzzers	0.873237		0.1	NaN	0.0	0.000000	Fuzzers	0.963769		0.42039	0.357247	0.319173	0.321097
Generic	0.873237		0.1	NaN	0.0	0.000000	Generic	0.963769		0.42039	0.987042	0.974678	0.980808
Reconnaissance	0.873237		0.1	NaN	0.0	0.000000	Reconnaissance	0.963769		0.42039	0.560558	0.650585	0.599229
Shellcode	0.873237		0.1	NaN	0.0	0.000000	Shellcode	0.963769		0.42039	0.000000	0.000000	0.000000
Worms	0.873237		0.1	NaN	0.0	0.000000	Worms	0.963769		0.42039	0.069811	0.074762	0.062739
Normal	0.873237		0.1	0.873237	1.0	0.932329	Normal	0.963769		0.42039	0.991638	0.988117	0.989862

Bagging, Adaptive Boosting, MLP e Random Forest

	Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1		Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1		
Analysis	0.979068		0.510448	0.609618	0.023673	0.044621	Analysis	0.983547		0.584948	0.871317	0.121515	0.212761
Backdoors	0.979068		0.510448	0.644488	0.059450	0.106346	Backdoors	0.983547		0.584948	0.817051	0.097931	0.174462
DoS	0.979068		0.510448	0.417983	0.330088	0.273759	DoS	0.983547		0.584948	0.309749	0.235063	0.267138
Exploits	0.979068		0.510448	0.658738	0.766836	0.687759	Exploits	0.983547		0.584948	0.631257	0.824145	0.714890
Fuzzers	0.979068		0.510448	0.670194	0.437320	0.523099	Fuzzers	0.983547		0.584948	0.779630	0.683635	0.728400
Generic	0.979068		0.510448	0.993927	0.983560	0.988716	Generic	0.983547		0.584948	0.997990	0.987289	0.992611
Reconnaissance	0.979068		0.510448	0.819709	0.754799	0.784980	Reconnaissance	0.983547		0.584948	0.925980	0.780141	0.846814
Shellcode	0.979068		0.510448	0.515739	0.508747	0.504477	Shellcode	0.983547		0.584948	0.844426	0.901570	0.871401
Worms	0.979068		0.510448	0.360000	0.242540	0.221685	Worms	0.983547		0.584948	0.644286	0.219683	0.323480
Normal	0.979068		0.510448	0.994035	0.997467	0.995748	Normal	0.983547		0.584948	0.997471	0.998512	0.997991

Resultados

— □ ×

Extreme Gradient Boosting

	Acurácia no Teste	Acurácia Balanceada no Teste	Precisão	Recall	F1
Analysis	0.98352	0.610389	0.848095	0.084735	0.153981
Backdoors	0.98352	0.610389	0.893626	0.096329	0.173710
DoS	0.98352	0.610389	0.434234	0.300773	0.355235
Exploits	0.98352	0.610389	0.650545	0.864893	0.742513
Fuzzers	0.98352	0.610389	0.746045	0.604409	0.667615
Generic	0.98352	0.610389	0.997497	0.987327	0.992386
Reconnaissance	0.98352	0.610389	0.921843	0.787112	0.849157
Shellcode	0.98352	0.610389	0.878125	0.906155	0.891304
Worms	0.98352	0.610389	0.622240	0.474127	0.536058
Normal	0.98352	0.610389	0.996349	0.998032	0.997190

Por Nô

	Acurácia_Binário	Acurácia_Multiclasse	Acurácia_Balanceada_Binário	Acurácia_Balanceada_Multiclasse
Mean	0.99645	0.983481	0.991431	0.594525
		Precision_Mean	Recall_Mean	F1_Mean
	Normal	0.997781	0.998155	0.997968
	Attack	0.987262	0.984706	0.985982

Por Nô Pai

	Acurácia_Binário	Acurácia_Multiclasse	Acurácia_Balanceada_Binário	Acurácia_Balanceada_Multiclasse
Mean	0.996447	0.983456	0.991381	0.587681
		Precision_Mean	Recall_Mean	F1_Mean
	Normal	0.997765	0.998168	0.997966
	Attack	0.987347	0.984595	0.985968

Por Nível

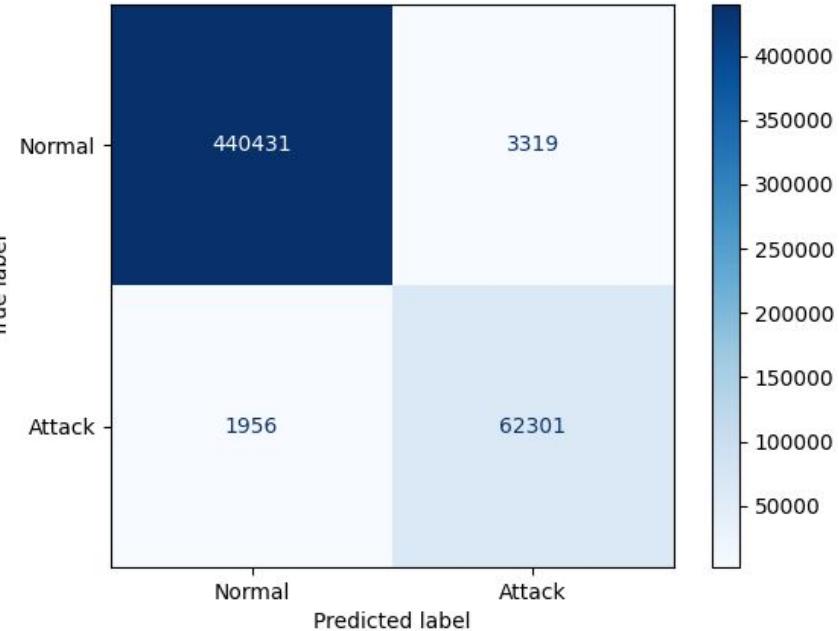
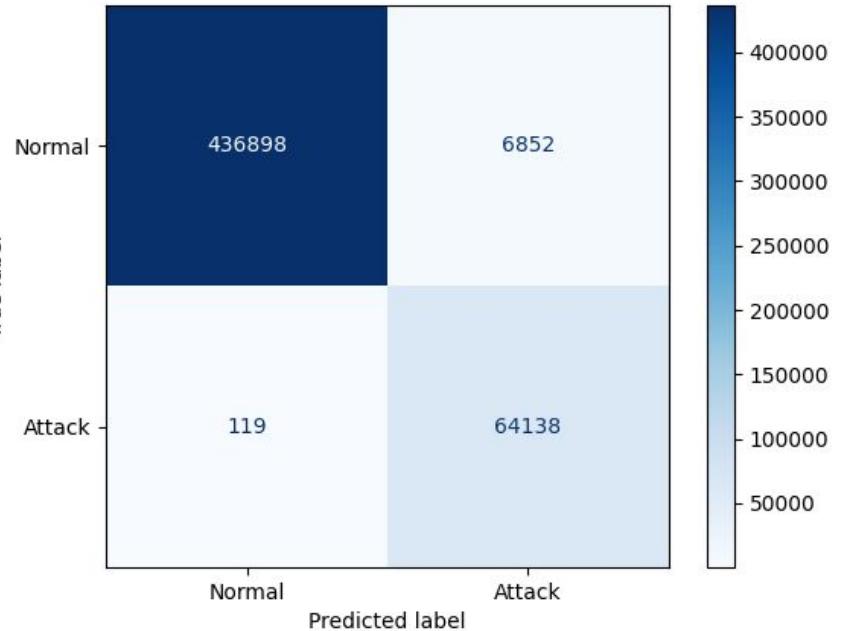
	Acurácia_Binário	Acurácia_Multiclasse	Acurácia_Balanceada_Binário	Acurácia_Balanceada_Multiclasse
Mean	0.996447	0.983427	0.991381	0.58719
		Precision_Mean	Recall_Mean	F1_Mean
	Normal	0.997765	0.998168	0.997966
	Attack	0.987347	0.984595	0.985968

	Precision_Mean	Recall_Mean	F1_Mean		Precision_Mean	Recall_Mean	F1_Mean
Analysis	0.817582	0.127165	0.219782	Analysis	0.851156	0.126527	0.219837
Backdoors	0.843748	0.103787	0.184486	Backdoors	0.891321	0.098019	0.176129
DoS	0.312674	0.239655	0.271189	DoS	0.314806	0.242599	0.273835
Exploits	0.630403	0.824973	0.714655	Exploits	0.630253	0.823923	0.714164
Fuzzers	0.757627	0.699358	0.727214	Fuzzers	0.757163	0.698749	0.726685
Generic	0.997945	0.987798	0.992845	Generic	0.997898	0.987429	0.992635
Reconnnaissance	0.928426	0.779149	0.847249	Reconnnaissance	0.928417	0.781137	0.848419
Shellcode	0.868891	0.900768	0.884078	Shellcode	0.845588	0.900579	0.871759
Worms	0.564286	0.284444	0.376370	Worms	0.603175	0.219683	0.319201
Normal	0.997781	0.998155	0.997968	Normal	0.997765	0.998168	0.997966

Por Nível, Por Nível Pai e Por Nível

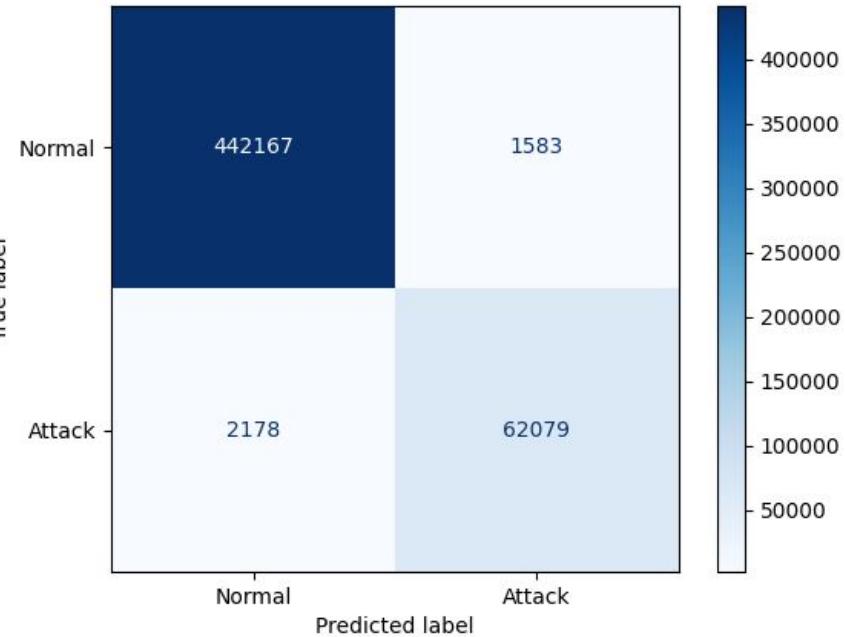
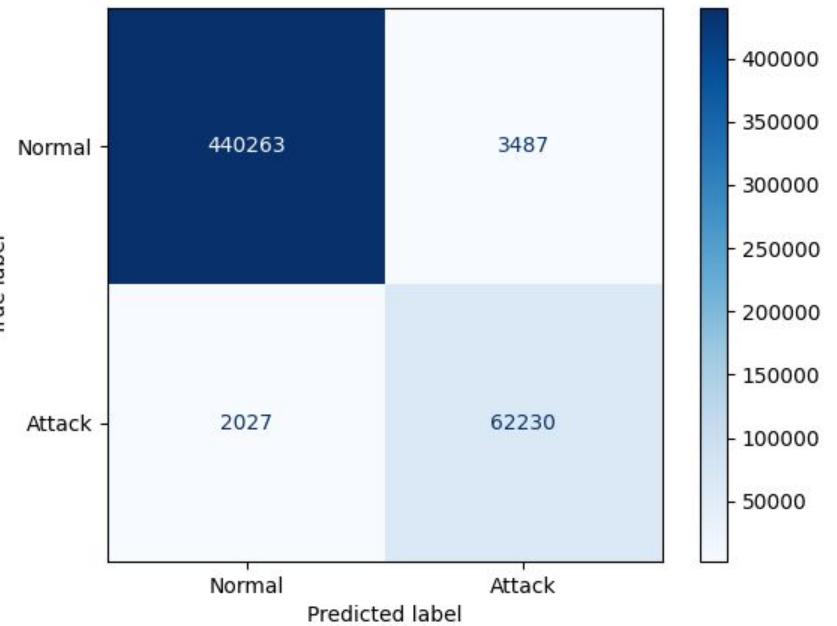
	Precision_Mean	Recall_Mean	F1_Mean
Analysis	0.824467	0.126545	0.218778
Backdoors	0.817051	0.097931	0.174462
DoS	0.309394	0.235067	0.267005
Exploits	0.628746	0.826129	0.714019
Fuzzers	0.761097	0.697845	0.728005
Generic	0.997990	0.987326	0.992630
Reconnnaissance	0.925832	0.780283	0.846838
Shellcode	0.841262	0.902922	0.870382
Worms	0.644286	0.219683	0.323480
Normal	0.997765	0.998168	0.997966

Bagging



Adaptive Boosting

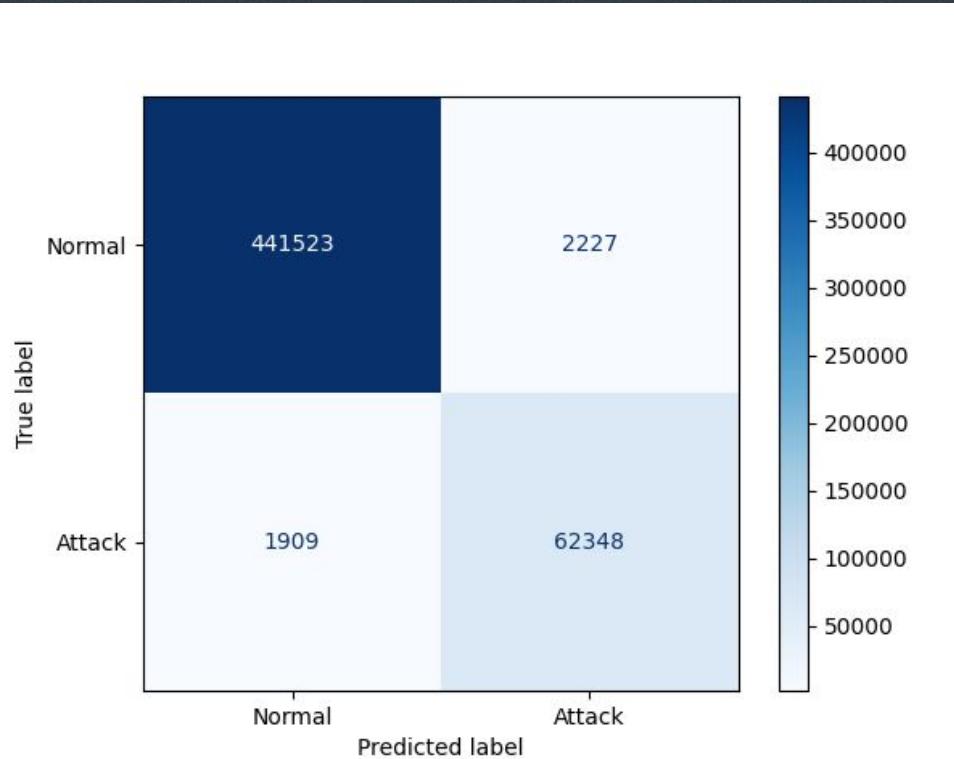
MLP



Random Forest

Extreme Gradient Boosting

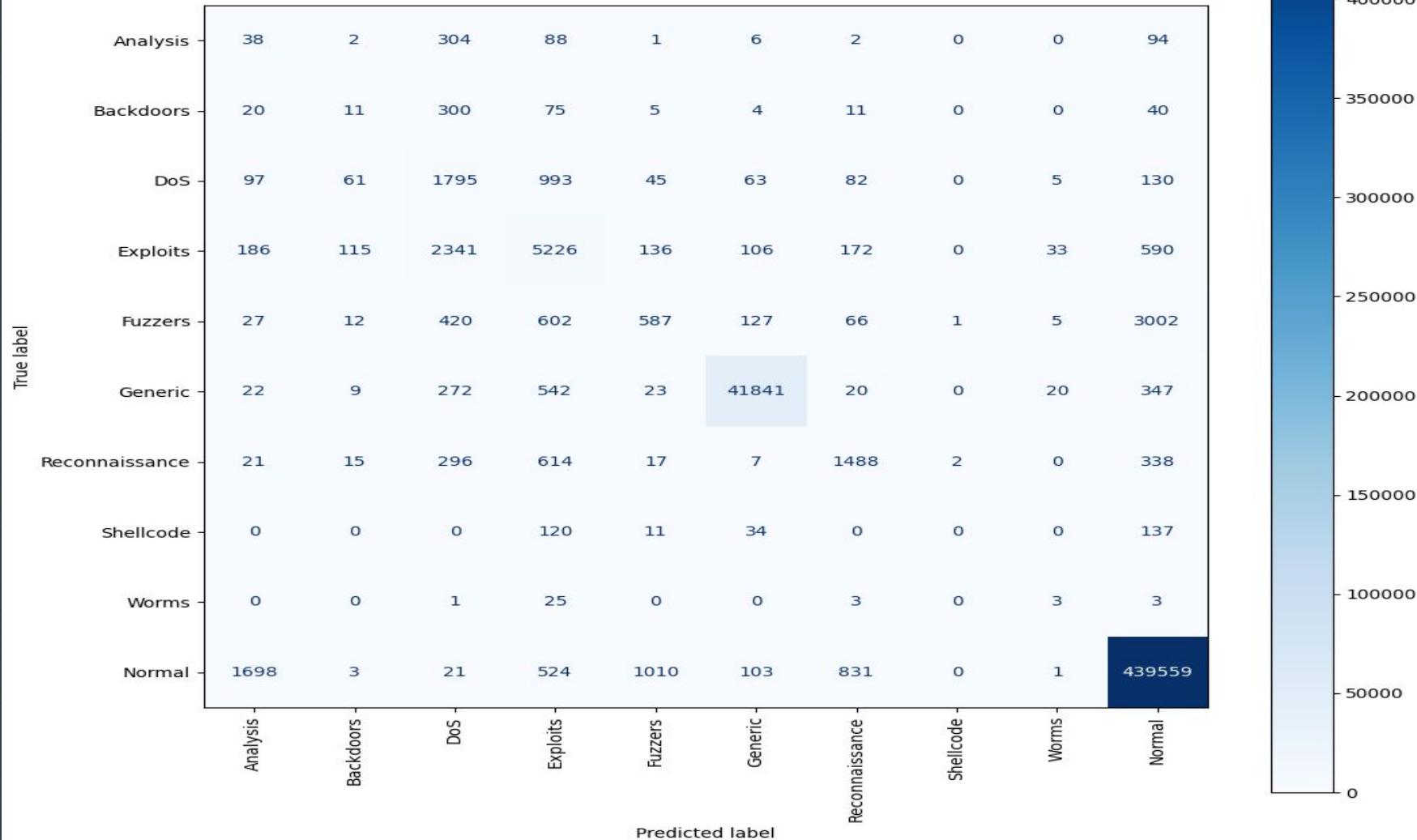
— □ ×



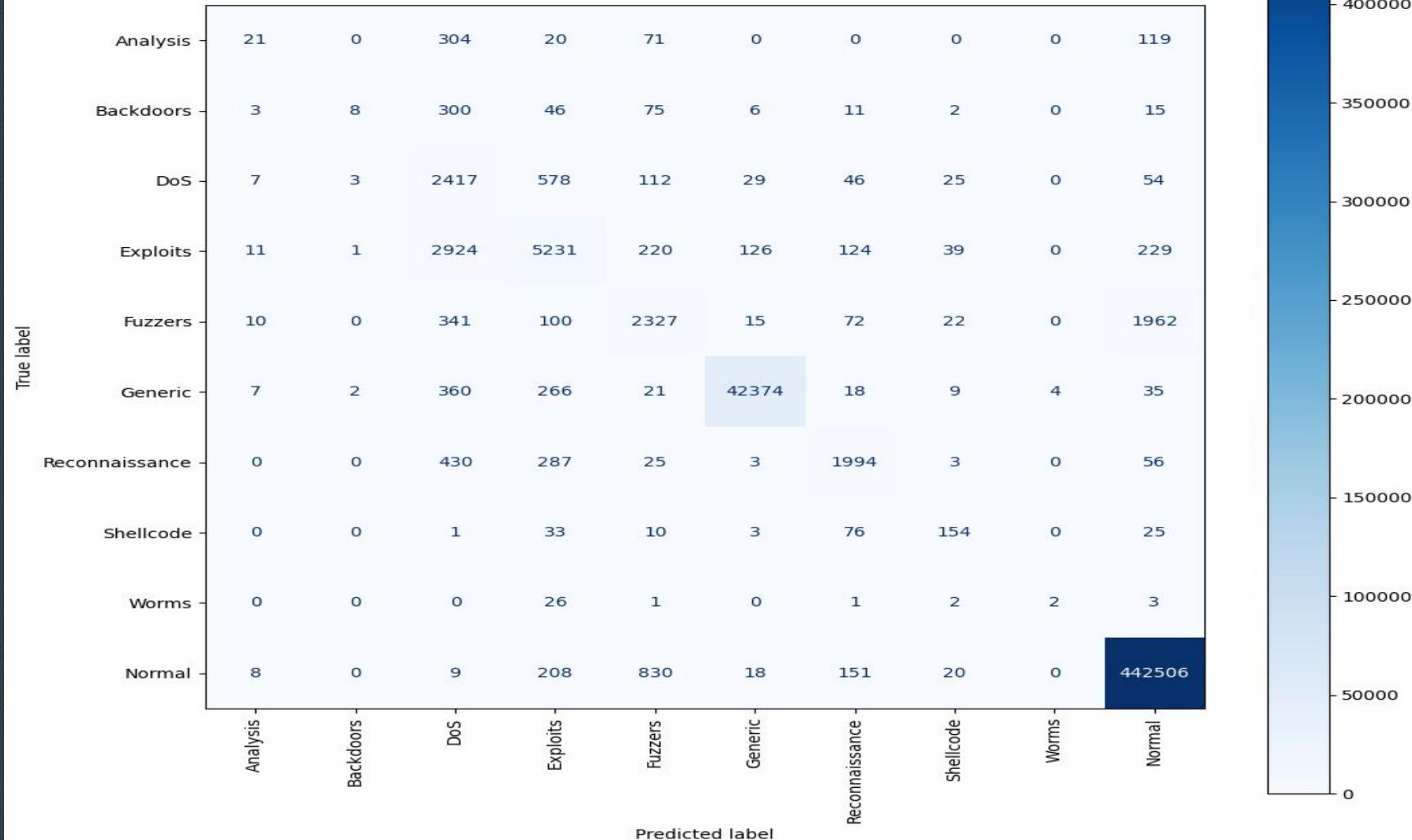
Bargaining



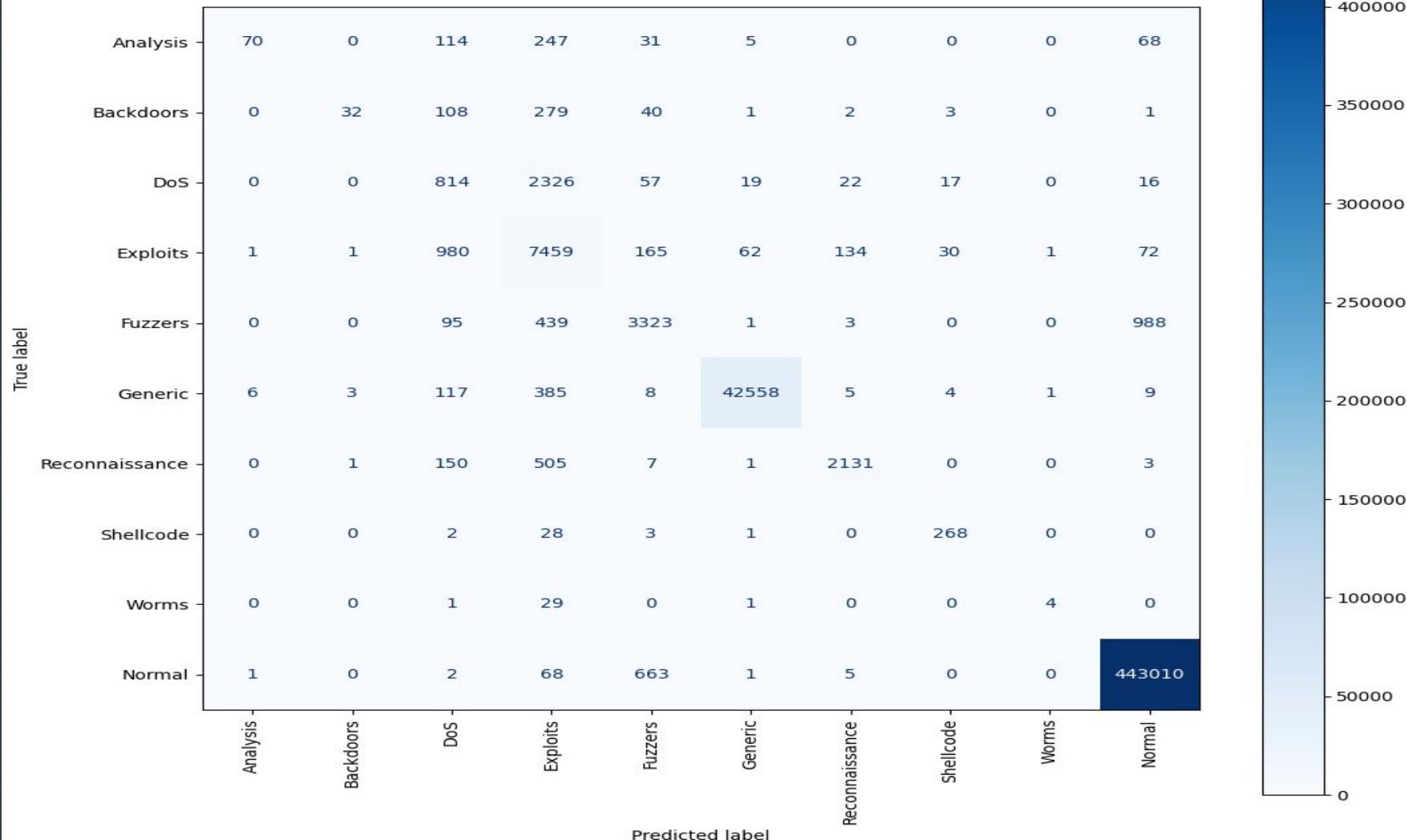
Adaptive Boosting



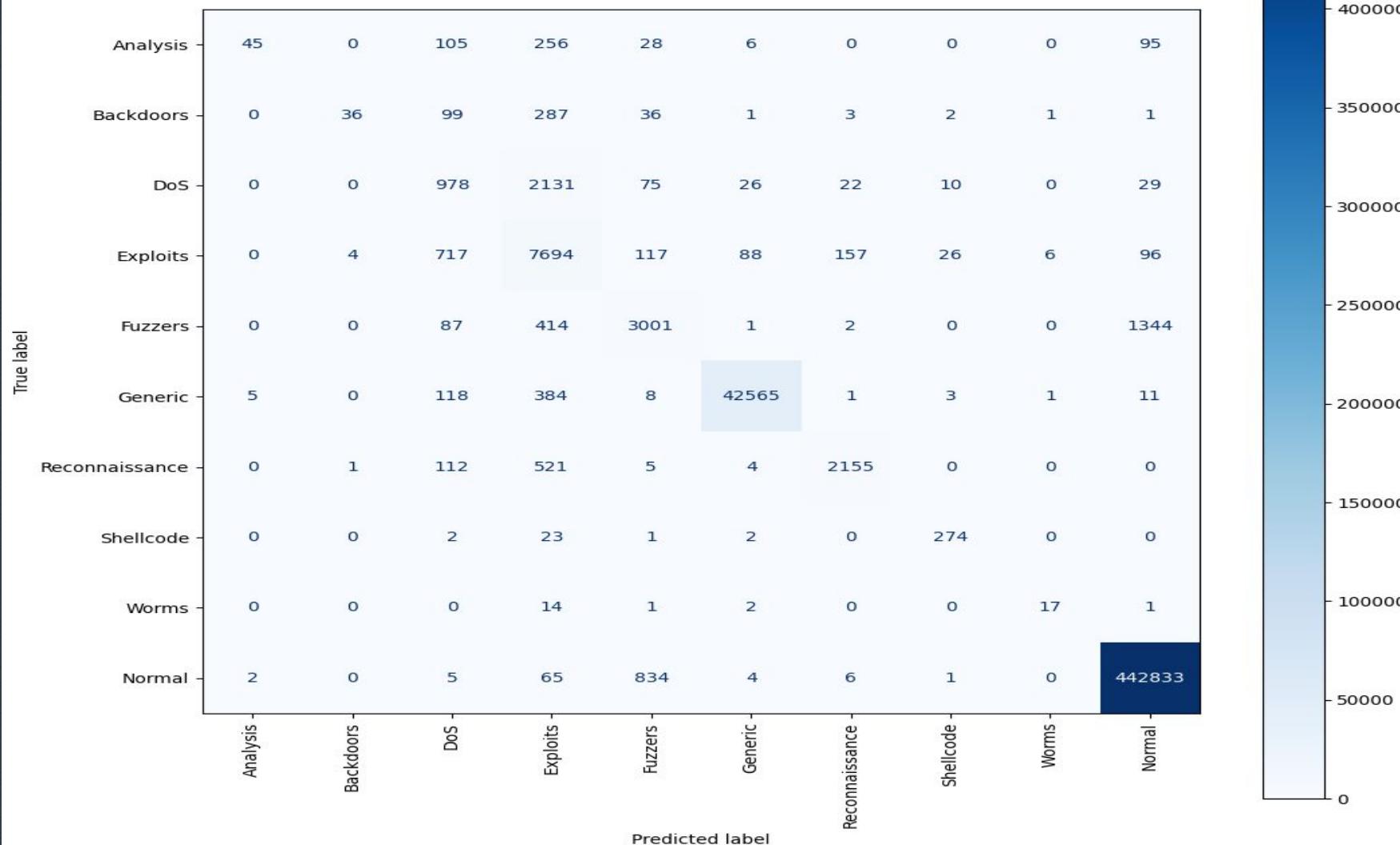
MLP

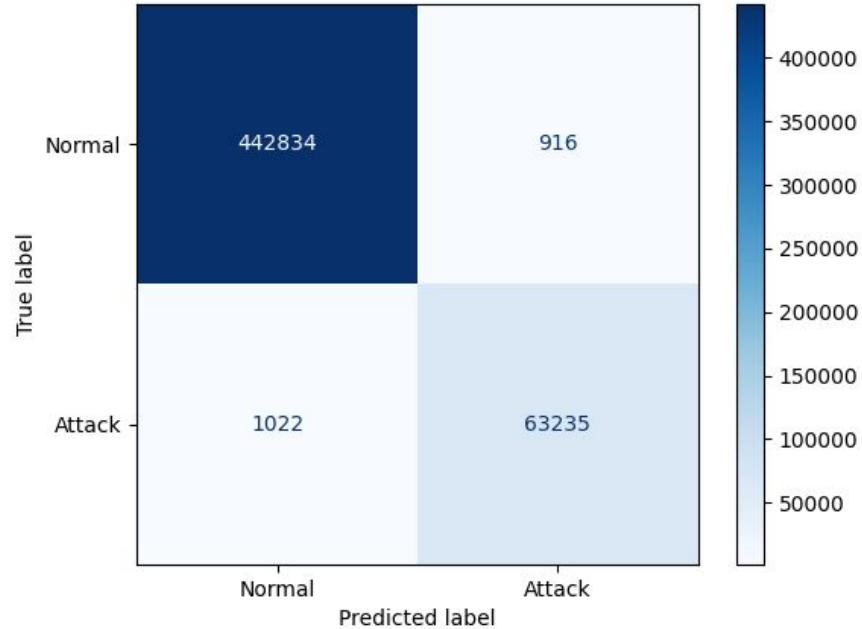
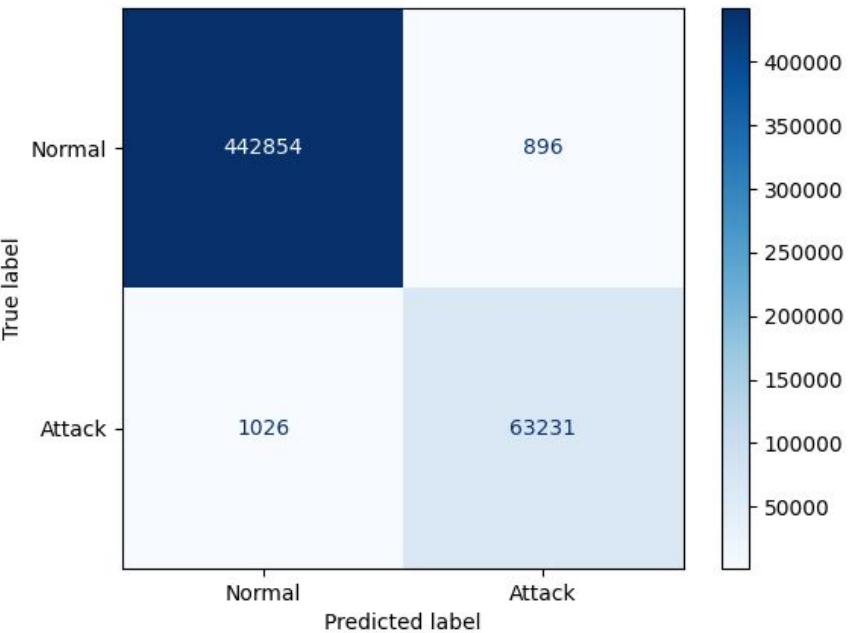


Random Forest



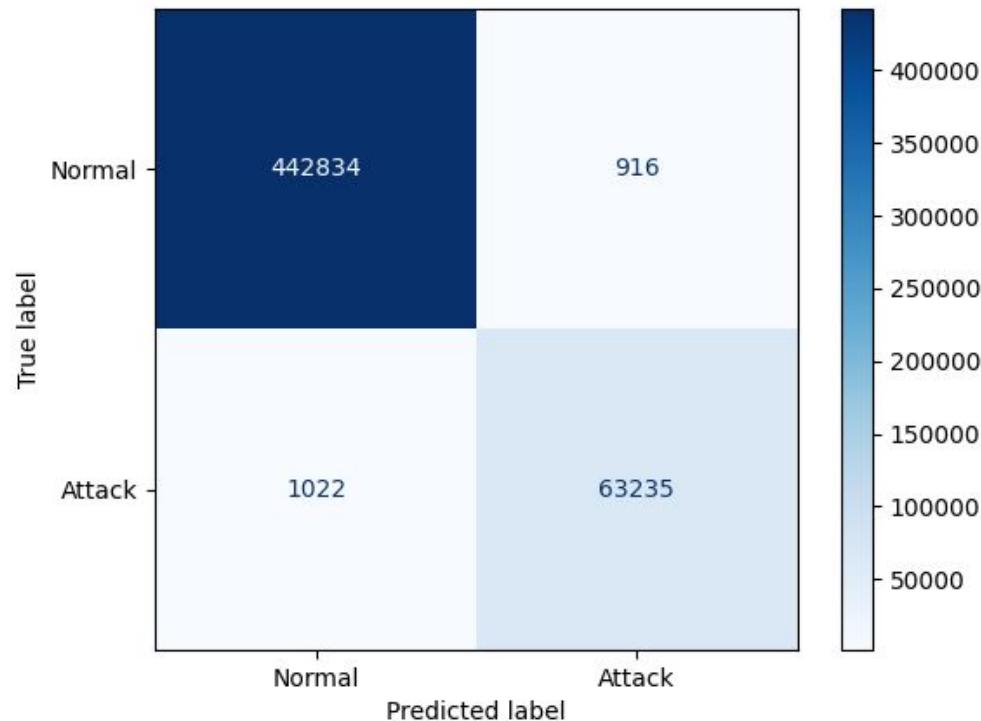
Extreme Gradient Boosting



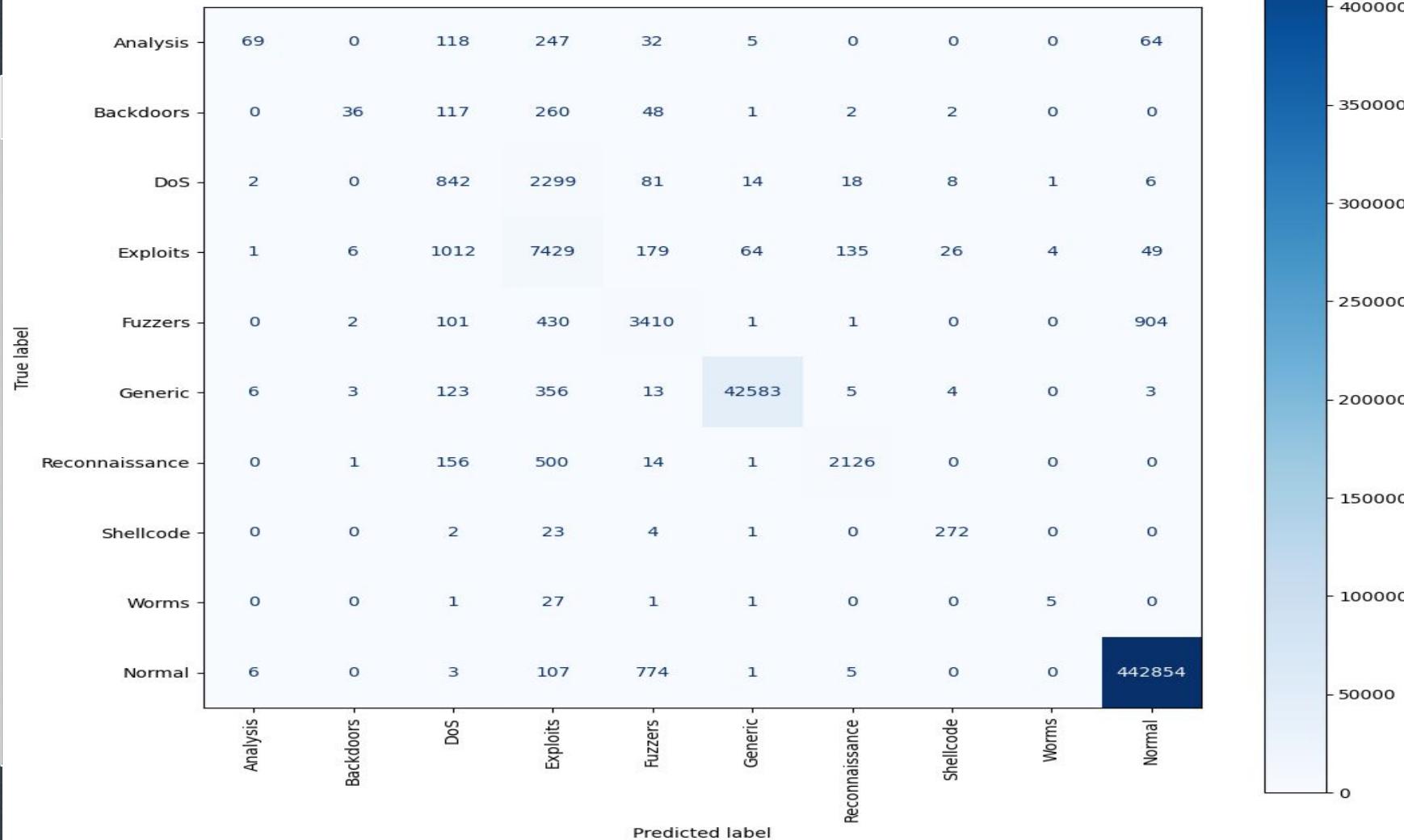


Por Nível

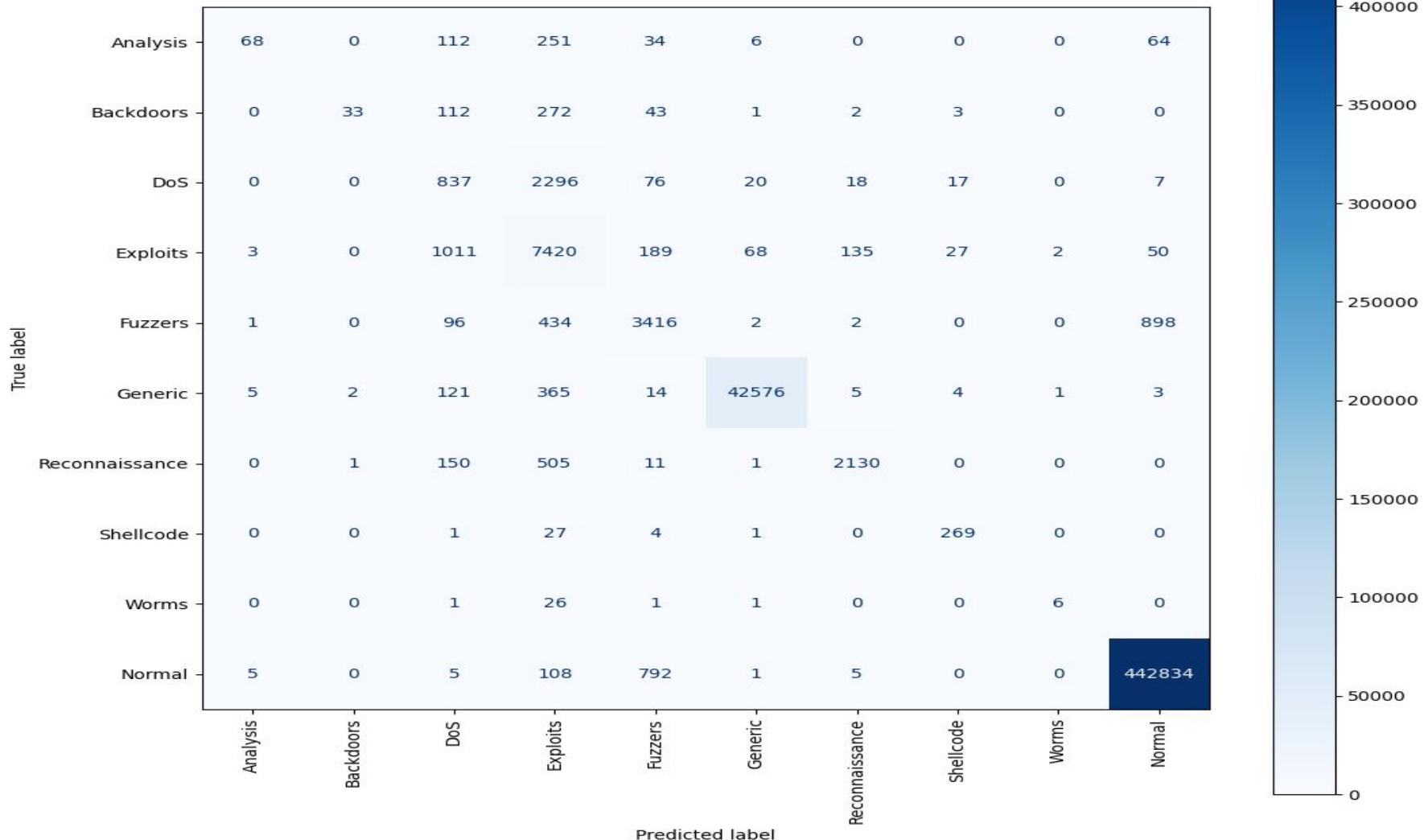
— □ ×



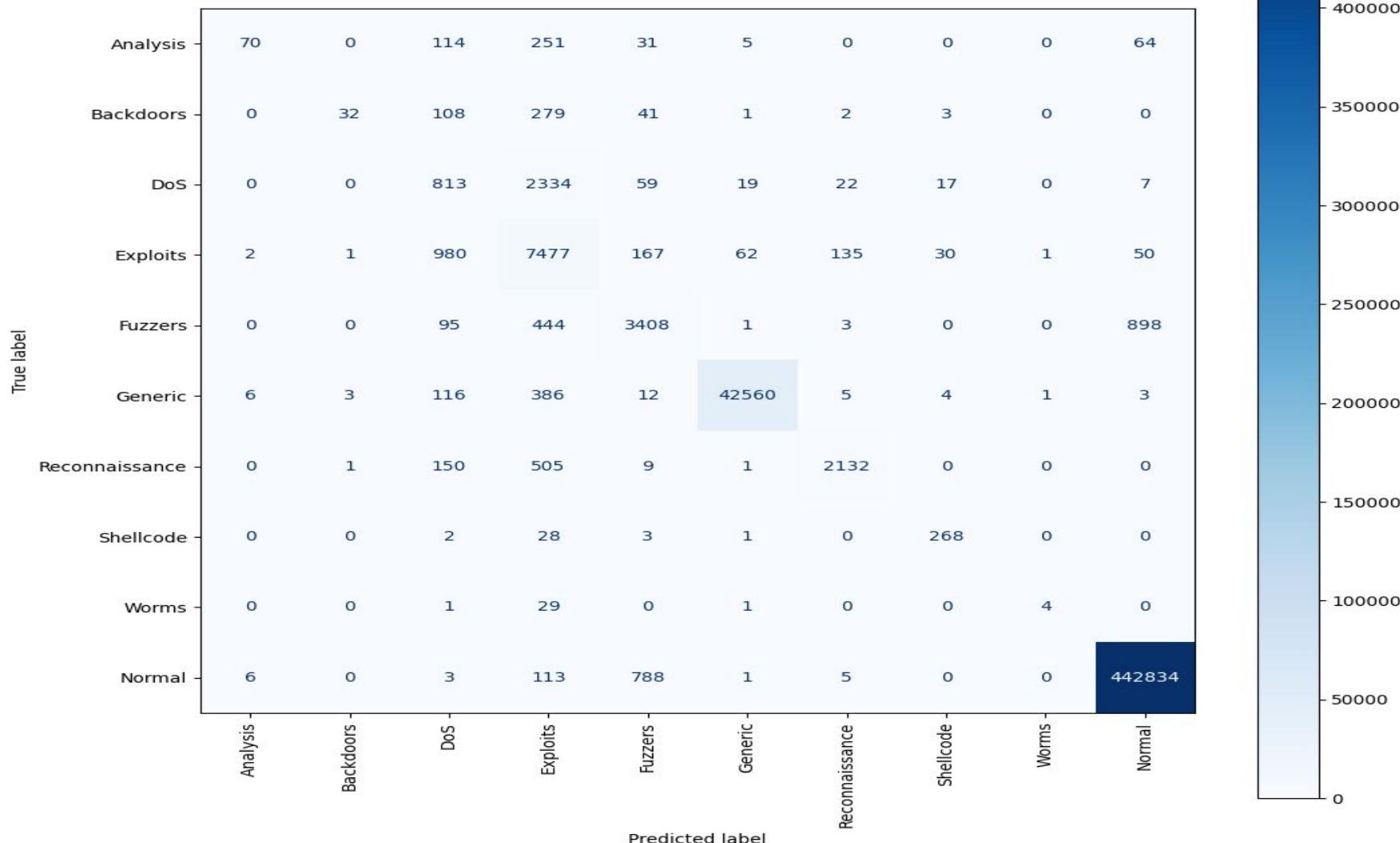
Por Nó



Por Nô País



Por Nível



Conclusão

— □ ×

- Modelos mais satisfatórios:
Extreme Gradient Boosting,
Random Forest e
Hierárquicos

— □ ×

← +

— □ ×

= > ⊕

Obrigado!

Você tem alguma pergunta?

— □ ×

÷ ▷

CRÉDITOS: Este modelo de apresentação foi criado pela [Slidesgo](#), e inclui ícones do [Flaticon](#) e imagens da [Freepik](#).

Referências:

- CHANG, Brittany. One of the biggest US insurance companies reportedly paid hackers \$40 million ransom after a cyberattack. *Business Insider*. Disponível em: <https://www.businessinsider.com/cna-financialhackers-40-million-ransom-cyberattack-2021-5>
- AXELSSON, Stefan. *Intrusion Detection Systems: A Survey and Taxonomy*. CiteSeer. Abril, 2000.
- RAKSHE, Tushar. GONJARI, Vishal. *Anomaly based Network Intrusion Detection using Machine Learning Techniques*. *International Journal of Engineering Research & Technology (IJERT)*. Maio, 2017.
- AKASHI SATO, Felipe Yuzo. *Análise do Desempenho de Algoritmos Classificadores para Detecção de Anomalias em Sistemas de Detecção de Intrusão*. Universidade Tecnológica Federal do Paraná (UTFPR). Junho, 2023.
- Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." *Military Communications and Information Systems Conference (MilCIS)*, 2015. IEEE, 2015.

Referências:

- Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set." *Information Security Journal: A Global Perspective* (2016): 1-14.
- MIRANDA, Fabio M. KO¹ HNECKE, Niklas. RENARD, Bernhard Y. HiClass: a Python Library for Local Hierarchical Classification Compatible with Scikit-learn. Janeiro, 2023.