Aplicação do algoritmo Random Forest para classificação de tráfego de rede benigno em meio a ataques DDoS UDP.*

Davi Jorge Leite Santos[1]
Felipe Augusto Lima Reis (Orientador)[2]

Resumo

Neste ano de 2023, houve um notável aumento no tráfego utilizado pelas operadoras e clientes, conforme observado nos registros do IX.BR. O aumento no volume de tráfego pode ter sido acompanhado por ataques de negação de serviço (DoS), como os DDoS distribuídos. Esse cenário requer monitoramento e análise contínuos. O protocolo NetFlow é empregado para coletar e armazenar informações em um banco de dados extenso. Para analisar esses dados, o algoritmo de aprendizado de máquina Random Forest é uma ferramenta viável para lidar com possíveis ataques. Uma análise exploratória do comportamento das informações coletadas pelo NetFlow é essencial para treinar o algoritmo de forma adequada, seguido por testes para avaliar sua precisão. Isso permite a classificação do tráfego como ataque ou benigno, buscando restabelecer o fluxo normal na rede. Em um conjunto específico de experimentos, o algoritmo Random Forest obteve uma acurácia de 83% na classificação de dados benignos em cenários de ataques DDoS.

Palavras-chave: Ataques de Negação de Seviço; DoS; Aprendizado de Máquinas. Inteligencia Artificial. Random Forest. Árvores de Decisão. Netflow.

*Trabalho de conclusão de curso, Sistemas de Informação, Unidade São Gabriel

[1]Programa de Graduação em Sistema da informação da PUC Minas, Brasil– davi.jls@outlook.com
[2]Instituto de Ciências Exatas e de Informática da PUC Minas, Brasil– felipereis@pucminas.br

Abstract

In this year of 2023, there has been a notable increase in traffic used by both carriers and customers, as observed in the records of IX.BR. The surge in traffic volume might have been accompanied by denial-of-service (DoS) attacks, such as distributed denial-of-service (DDoS). This scenario necessitates continuous monitoring and analysis. The NetFlow protocol is employed to gather and store information in an extensive database. To analyze this data, the machine learning algorithm, Random Forest, emerges as a viable tool to handle potential attacks. An exploratory analysis of the behavior of information collected by NetFlow is essential to appropriately train the algorithm, followed by tests to assess its accuracy. This facilitates the classification of traffic as either attack or benign, aiming to restore normal flow within the network. In a specific set of experiments, the Random Forest algorithm achieved an 83% accuracy in classifying benign data within DDoS attack scenarios.

Keywords: AI. Artificial Intelligence. Netflow. Machine Learning. Reinforcement Learning Algorithm. CNN. RL. Denial-of-Service attacks. DoS. Netflow.

1 INTRODUÇÃO

Este artigo emprega o algoritmo Random Forest, um método de aprendizado de máquina, para detecção e prevenção de ataques de Negação de Serviço (DoS). A escolha deste método foi embasada em estudos anteriores que exploraram diversos algoritmos de classificação, incluindo o Random Forest, para identificar o tráfego de entrada em um ambiente SDN (AL-DUNAINAWI et al., 2023). Com o constante aumento do tráfego de rede em 2023, chegando a 31 Tbit/s de pico de tráfego no dia 13/07/2023 no Brasil, de acordo com IX.BR (Projeto do Comitê Gestor da Internet no Brasil), foi motivado o desenvolvimento de novas técnicas para análise dos incidentes e identificar padrões que possam indicar esses ataques, tal como o DoS (IX.BR, 2023).

Alem disso, até a data de 11/04/2023 os ataques baseados em UDP ficaram em terceiro lugar com 21% de participação em 2023, segundo a Cloudflare, reforçando a identificação e proteção das redes (YOACHIMIK; PACHECO, 2023). Baseados em um histórico de ataques, os algoritmos de Aprendizado de Máquina (Machine Learning - ML) podem ser treinados para a classificação desses ataques.

Uma das aplicações do aprendizado de máquina é analisar padrões de tráfego que indicam ocorrências de ataques DoS. Segundo o estudo de Lai et al. (2019), a IA tem sido eficaz na detecção e prevenção de ataques DoS, alcançando uma precisão media de 95.075% (No caso apresentado, temos quatro métodos: SVM ensemble method (94.5%), HMM (93.4%), Decision tree method (93.1%) e Our method (99.3%). Somando essas acurácias, obtemos 380.3. Dividindo esse total pelo número de métodos (4), obtemos uma média de acurácia de 95.075%). Com a capacidade de analisar grandes volumes de dados em tempo real, os algoritmos de IA conseguiram identificar padrões de tráfego indicativos de um ataque.

Como resultado, seu uso pode contribuir para aumentar a segurança cibernética e minimizar o impacto dos ataques DoS. O tráfego benigno, no contexto do ataque DDoS, seria toda informação usual, sem o intuito de derrubar o serviço, além de utilizar portas padrões da internet, assim como seus serviços. Tais serviços podem utilizar tanto protocolos UDP quanto TCP. E essas aplicações devem continuar funcionando, fazendo assim que seja necessário entender o comportamento do mesmo.

Para contribuir com a utilização da inteligência artificial e analisar o tráfego de ataques DoS a fim de prever os eventos, o artigo realizou testes em uma base de dados que continha um histórico de informações sobre ataques DDoS. O presente trabalho buscou responder a seguinte questão: **É possível utilizar um algoritmo do Random Forest para classificar o tráfego benigno, em meio a um ataque DDoS coletado pelo protocolo Netflow?**

O artigo visa analisar a utilização do algoritmo Random Forest no âmbito da cibersegurança para conseguir investigar um ataque DDoS do tipo inundação de UDP, utilizando uma base de dados coletada pelo protocolo Netflow e conseguir assim classificar o tráfego benigno.

O artigo tem os seguintes objetivos específicos: (i) verificar se o Random Forest será assertivo na classificação das informações Benignas; (ii) realizar análise exploratória da base de dados que contém trafego de rede UDP e verificar características do ataque DoS e DDoS, para metrificá-las para utilização do Random Forest; (iii) classificar o tráfego dos usuários benignos em meio a um ataque DoS, identificando-os do próprio ataque.

O estudo propõe uma técnica para detectar tráfego benigno em cenários de ataques DDoS UDP usando o algoritmo Random Forest, avaliando seu desempenho na manutenção da disponibilidade dos serviços dos clientes. É direcionado a empresas que gerenciam servidores, visando evitar quedas de serviço e, consequentemente, reduzir custos relacionados à identificação desses ataques.

O trabalho visa contribuir na área de cibersegurança e detecção de ataques DDoS, assim como na distinção de tráfego benigno. Suas principais contribuições são:

1) Detecção e prevenção de ataques DoS e DDoS com o algoritmo Random Forest: O estudo foca na aprimorada segurança cibernética para classificação de dados benignos. Ao demonstrar a eficácia do algoritmo Random Forest na detecção de ataques DDoS, visa fortalecer as defesas cibernéticas de organizações, proteger ativos críticos e serviços essenciais, mantendo o tráfego legítimo. A avaliação será realizada por meio de experimentos comparativos com outros métodos existentes na literatura.

2) Redução de Riscos: O estudo busca reduzir riscos através do uso eficiente do Random Forest na detecção de ataques DDoS ou tráfego benigno, medindo essa eficácia por indicadores como a acurácia.

3) Progresso na Compreensão da Cibersegurança: Visa aprimorar a compreensão da cibersegurança, especialmente nos ataques de negação de serviço. Identificar métricas relevantes e estratégias analíticas eficazes busca ampliar o conhecimento científico e incentivar pesquisas futuras na área. Isso será demonstrado por meio de uma análise exploratória dos dados do protocolo Netflow, extraindo características e padrões dos ataques e do tráfego benigno.

Essas áreas representam as contribuições principais, abrangendo aspectos práticos e teóricos da cibersegurança e detecção de ataques DoS, incluindo o tráfego benigno.

2 REFERENCIAL TEÓRICO

Nesta seção, serão explorados conceitos fundamentais relacionados à segurança cibernética e à inteligência artificial.

2.1 Ataques de Negação de Serviço Distribuído (DDoS)

Um ataque DoS (Denial of Service) é direcionado a um único dispositivo ou recurso, buscando consumir seus recursos para interromper a disponibilidade do serviço ou da rede. Em contraste, o ataque DDoS (Distributed Denial of Service) coordena múltiplos dispositivos para atacar simultaneamente, aumentando consideravelmente o volume de tráfego (SILVA; SALLES, 2015).

O DDoS tem como objetivo interromper ou reduzir a disponibilidade de um serviço na internet, podendo afetar transações e tornar empresas e seus produtos indisponíveis. Ao sobrecarregar serviços conectados à internet, utilizando uma rede de computadores interligados, o DDoS prejudica a disponibilidade para os usuários (SILVA; SALLES, 2015).

Essa ameaça à segurança cibernética pode interromper serviços online e afetar recursos críticos na web, causando mau funcionamento e indisponibilidade do sistema (SILVA; SALLES, 2015). O ataque envolve vários computadores enviando requisições a uma página ou conexão, resultando em lentidão ou parada do serviço. Considerando essa possível negação de serviço, é classificado como uma vulnerabilidade, pois todos os serviços são suscetíveis a isso (SILVA; SALLES, 2015).

Métodos identificados para detectar esses ataques incluem detecção por assinatura, que requer conhecimento de padrões presentes em pacotes maliciosos, e detecção por anomalia, baseada em comportamentos de tráfego de rede em condições normais, estabelecendo limites para identificar ataques (SILVA; SALLES, 2015).

2.2 Análise de Dados e Inteligência Artificial

O aumento do tráfego devido ao DDoS demanda métodos para identificar anomalias. Algoritmos de aprendizado de máquina são usados para classificar e generalizar essas ocorrências, gerando conhecimento para identificar o problema.

O objetivo é capacitar os computadores a aprender com os dados fornecidos. O processo inicia-se com o treinamento de algoritmos especializados que realizam previsões baseadas nos dados utilizados para seu treinamento. Essas previsões antecipam ações e eventos (RAJA et al., 2022).

A aplicação de modelos analíticos de aprendizado de máquina para prevenção e predição de redes hostis pode aprimorar os modelos de IA e ML, beneficiando diversos setores de redes ao agilizar diagnósticos e minimizar vieses humanos (SILVA; SALLES, 2015). Destaca-se a importância do processamento para aprimorar a capacidade dos modelos de previsão na detecção de ataques, otimizando os procedimentos de diagnóstico (SILVA; SALLES, 2015).

2.3 Utilização do Protocolo Netflow para Coleta de Dados

DoS e DDoS são comuns na cibersegurança, podendo causar lentidão e interrupção nos serviços de internet. O protocolo Netflow da Cisco permite o monitoramento em tempo real do tráfego de rede, coletando informações cruciais para ajustes e respostas a possíveis ataques. Esses dados são usados por algoritmos de detecção de DoS para analisar padrões de tráfego e identificar possíveis ameaças. O Netflow também é empregado na coleta e armazenamento de dados de tráfego para posterior processamento, permitindo a extração de informações relevantes sobre ataques DDoS. A detecção pode ser realizada por meio de aprendizado de máquina ou roteiros personalizados sem aprendizado (SILVA; SALLES, 2015).

2.4 Árvore de Decisão e Random Forest

A Árvore de Decisão é um algoritmo de aprendizado de máquina que organiza e representa dados usando classificadores binários em um formato de árvore. Esse modelo toma decisões baseadas em características, ramificando-se e considerando múltiplos atributos até a classificação. A métrica, como o índice Gini ou Entropia, é usada para classificar e selecionar atributos nos nós da árvore (OKADA et al., 2023). O Índice Gini mede a impureza dos elementos, enquanto a Entropia avalia a imprevisibilidade e desordem nos dados (SILVA, 2005). O Overfitting ocorre quando a árvore se ajusta excessivamente aos dados de treinamento, sendo crítico em árvores de decisão, resultando em classificações superprecisas (SILVA, 2005).

O algoritmo Random Forest, uma variação da Árvore de Decisão, emprega múltiplas árvores com características aleatórias para aumentar a precisão na classificação. Combinação de várias Árvores de Classificação torna as classificações mais robustas e precisas, reduzindo a probabilidade de overfitting (CHEN et al., 2023).

3 TRABALHOS RELACIONADOS

Nesta seção serão apresentados trabalhos que realizaram pesquisas sobre inteligência artificial no contexto de cibersegurança e proteção de serviços.

3.1 Análise do Tráfego de Rede

O estudo de Kemp et al. (2021) destaca que o aumento do volume de dados transmitidos em rede intensifica a tentativa de coleta não autorizada de informações. A análise de metadados do tráfego de rede é proposta para identificar anomalias e vulnerabilidades. Características específicas do tráfego, consideradas metadados, são usadas para detectar anomalias e permitir

ações preventivas contra agentes mal-intencionados. O aprendizado de máquina é empregada para analisar os metadados e identificar ameaças seguramente (KEMP et al., 2021).

O artigo Hou et al. (2018) destaca que os métodos tradicionais de detecção de DDoS, por assinatura e por anomalia, são mais manuais e baseados em roteiros de comandos.(HOU et al., 2018). Os resultados apresentados, indicam uma alta taxa de acurácia, 99%, após a extração dos dados do Netflow, com baixa incidência de falsos positivos, tornando o detector confiável para uso, especialmente com dados amostrados, indicado pelo Hou et al. (2018).

3.2 Aprendizado Profundo para Sistemas de Detecção de Intrusão de Redes (NIDS)

O trabalho apresentado por Corsini et al. (2021) comenta que irá demonstrar interesse em Aprendizado Profundo para Sistemas de Detecção de Intrusão de Redes (NIDS) que terão por meio de abordagens sequenciais, a capacidade de extrair informações temporais dos fluxos de tráfego de rede (Netflow), apresentam potencial para contribuir com a área da cibersegurança. O artigo propôs um problema detalhado onde a metodologia para extrair essas sequências temporais, como comparação para o modelo de aprendizado, tal como modelos tradicionais e estáticos (CORSINI et al., 2021).

O autor realiza algumas comparações de modelos como Short-Term Memory (LSTM) contra um modelo "estático" de Feedforward Neural Networks (FNN) em dois conjuntos de dados bem conhecidos para NIDS: o CICIDS2017 (SHARAFALDIN et al., 2018) e o CTU13 (GARCíA et al., 2014). algoritmo alcançou uma precisão de 95%, similar à precisão de 96% alcançada pelo FNN no CICIDS2017, conforme reportado por Corsini et al. (2021).

3.3 Classificação de Metadados de Tráfego de Rede e Segurança Cibernética

O trabalho conduzido por Watkins et al. (2021) descreveu um crescente volume de informação digital e o aumento correspondente nas tentativas de roubo de dados. Destacou-se a importância de estabelecer uma forma segura de identificar características típicas do ataques de modo a evitar desvios nos dados, considerando a possibilidade de roubo de informações sem detecção. O artigo enfatizou o desenvolvimento de uma abordagem de IA para classificar e analisar metadados do tráfego de rede, visando determinar suas características e níveis de segurança (WATKINS et al., 2021). Adicionalmente, o estudo apontou a implementação bem-sucedida do modelo em uma rede dinâmica do mundo real para classificação de segurança, ressaltando os benefícios do aprendizado de máquina (WATKINS et al., 2021).

3.4 Detecção de Anomalias em Tráfego de Rede com Algoritmos de Classificação de Machine Learning

No trabalho de Fosić et al. (2023), foram explorados vários algoritmos de classificação de machine learning, como Stochastic Gradient Descent (SGD), Support Vector Machines (SVM), K-Nearest Neighbor (K-NN), Gaussian Naive Bayes (GNB), Decision Tree (DT), Random Forest (RF) e AdaBoost (AB), para a detecção de anomalias no tráfego de rede. O estudo utilizou o conjunto de dados UNSW-NB15 e evidenciou que o classificador obteve resultados com F2-score = 97,68% e AUC score = 98,47%. Além disso, o trabalho apresentou uma abordagem única, focando na otimização dos processos de machine learning, na redução de recursos e na adoção de vários métodos de codificação de recursos categóricos para aprimorar a análise (FOSIć et al., 2023).

3.5 Detecção de Anomalias no Tráfego de Rede com Foco no Ataque DDoS

O estudo conduzido por Mekala e Dasari (2023) se concentrou na área de cibersegurança, visando a seleção dos melhores algoritmos de detecção de anomalias para o fluxo de dados do Netflow. Ao reduzir os recursos utilizados em 82% e explorar diferentes recursos de categorias. O artigo contribui para a compreensão e a melhoria da detecção de anomalias no tráfego de rede, promovendo a segurança cibernética (MEKALA; DASARI, 2023).

Utilizando o conjunto de dados CIC-DDoS2019 (CYBERSECURITY, 2019), a pesquisa focou em analisar o tráfego DDoS, especialmente na área do Netbios, através do aprendizado de máquina. Destacou-se o uso do algoritmo Random Forest como um método para identificar e filtrar o tráfego DDoS com eficácia (CHEN et al., 2023). O modelo implementado no Spark alcançou uma Taxa de Falsos Positivos (FPR) de 0,0% e uma Taxa de Falsos Negativos (FNR) de 4,36%, buscando precisão na detecção. Trabalhos futuros estão direcionados para a extração de características e a implementação de um modelo de filtragem de tráfego em tempo real para prevenir ataques DDoS (CHEN et al., 2023).

3.6 Desafios e Possibilidades da IA na Segurança Cibernética

Segundo Das e Sandhane (2021), a IA é utilizada para detectar e aplicar modelos analíticos, organizando dados para treinamento e aumentando a acurácia preditiva, especialmente em locais com grandes volumes de dados. No entanto, essa crescente utilização da IA na defesa das informações também implica em novos desafios para a segurança física e lógica. Invasores cibernéticos podem usar ferramentas baseadas em IA para realizar ataques mais sofisticados e adaptativos. Além disso, a rápida evolução da IA pode gerar várias oportunidades que podem ser aproveitadas para fins positivos ou negativos. A tecnologia mais recente na compreensão,

interpretação e gestão de informações, especialmente na área de aprendizado de máquina, pode trazer benefícios para a segurança cibernética, mas também apresenta desafios e riscos de uso indevido. (DAS; SANDHANE, 2021).

4 METODOLOGIA

A metodologia utilizada foi composta por três etapas, sendo elas: análise exploratória, o treinamento do algoritmo e, por fim, a medição da acurácia do algoritmo na base de teste. Essas etapas compuseram o processo para a utilização dos algoritmos de aprendizado de máquina descritos no artigo.

Na primeira etapa, foi realizada a análise dos dados, visando fazer uma detecção por meio das anomalias apresentadas, e assim a compreensão do comportamento de cada informação e suas respectivas correlações. Essa compreensão foi essencial para a escolha de uma métrica adequada, utilizada na próxima etapa.

Posteriormente, passou-se para a fase de treinamento, na qual, após a seleção da melhor métrica, ocorreu a execução do algoritmo de Machine Learning escolhido, o Random Forest. Durante essa etapa, o algoritmo foi treinado, sendo determinadas as estratégias para a separação entre a base de treinamento e a base de teste.

Por fim, na última etapa, ocorreu o treinamento dos dados para verificar a acurácia do algoritmo em conjunto com o Macro AVG e Weighted AVG. Isso permitiu a avaliação da precisão do algoritmo proposto. Além disso, buscou-se compreender o momento e o local de início de um ataque em massa para o algoritmo poder aprender e classificar.

4.1 Bibliotecas e ferramenta utilizadas

A pesquisa de Insight-Lab (2023) destaca o Python como uma linguagem de programação globalmente popular, especialmente em aplicações de Data Science, segundo um levantamento do StackOverflow de 2018 (INSIGHT-LAB, 2023). Essa conclusão se baseia na extensa adoção do Python, em sua sintaxe clara e na presença de bibliotecas especializadas como Pandas, NumPy e Scikit-learn, sendo frequentemente escolhido para análise de dados. (INSIGHT-LAB, 2023)

A linguagem Python foi empregada no desenvolvimento da aplicação, juntamente com a biblioteca Jupyter-Lab. O Graphviz foi utilizado para exportar a árvore de decisão criada pelo Random Forest. O Pandas é uma ferramenta que faz o controle de matrizes e listas em um formato que ele chama de Dataframe, sendo responsável por toda a manipulação da base de dados, juntamente com o NumPy. O NumPy oferece estruturas de dados, como arrays multidimensionais e funções para operações rápidas e eficientes.

4.2 Base de dados

A base de dados utilizada foi o *DDoS Evaluation Dataset (CIC-DDoS2019)*, que contém dados de DDoS de diferentes tipos. Eles envolve conjuntos de recursos para detectar diferentes tipos de ataques DDoS, incluindo DDoS reflexivo (como DNS, LDAP, MSSQL, e TFTP), UDP, UDP-Lag e SYN (SHARAFALDIN et al., 2019).

A base de dados contém sub-datasets, relacionados a tipos diferentes de ataque. **Dentre os datasets existentes, foi selecionado o DrDoS-UDP, que contém ataques de DDoS relacionado a UDP**. Ela é composta por 3.136.802 linhas, contendo de registros de tráfego benigno ou de DDoS. As colunas consistem em valores numéricos, com exceção de "Label", no formato de texto, "Timestamp", no formato de data, e origem e destino dos pacotes, em formato de IP. (SHARAFALDIN et al., 2019)

O conjunto de dados utilizado contém informações coletadas pelo protocolo Netflow para armazenar ataques DDoS de diferentes tipos, incluindo o ataque de DDoS do tipo inundação de UDP. A coleta de dados começou às 09:40 UTC-4 e terminou às 17:35 UTC-4. A coleta de dados para o ataque de UDP começou às 12:36 UTC-4 e terminou às 13:04 UTC-4. A distribuição de informações na base de dados inclui 2.157 informações benignas e 3.134.645 dados de DDoS, relacionados a pacotes das camadas 3 e 4 do modelo TCP/IP, abrangendo aspectos como protocolo, tamanho do pacote, origem e destino. As colunas são todas relacionadas ao Netflow e às informações de pacotes presentes em protocolos de rede.

4.3 Treinamento e Testes

Foram realizados testes com a base de dados escolhida. Para treinamento do algoritmo, a base foi dividida em 75% para treinamento e 25% para testes.

5 EXPERIMENTOS E RESULTADOS

Inicialmente, foi feita a análise exploratória da base de dados, que teve um foco de entender o comportamento das informações existentes. Com base neste comportamento, foi executado um algoritmo de Aprendizado de Máquinas e por fim foi feita a avaliação dos resultados.

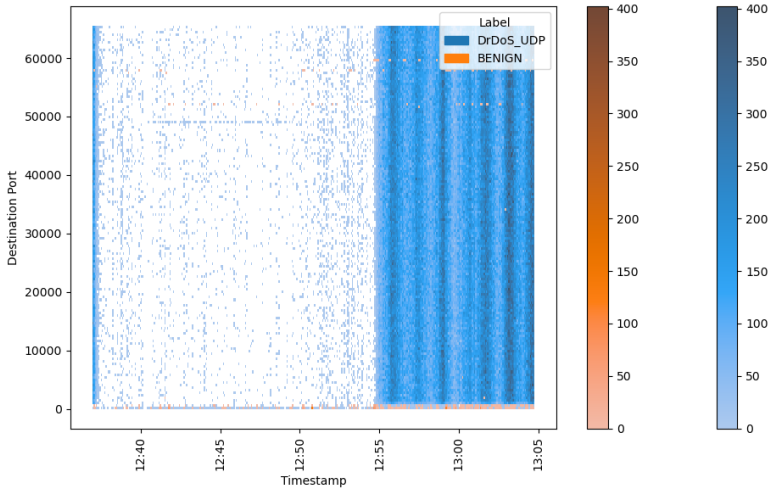
5.1 Análise exploratória

O algoritmo foi dividido em duas partes principais. A primeira corresponde ao pre-processamento dos dados, que executa uma série de tratamentos, utilizando conversões e verificando se está nas datas e horários abrangentes da base de dados. A segunda parte corresponde a própria apresentação, onde são apresentados gráficos para análise. Essa análise foi feita em no horário de 12:36 UTC-4 até o horário final de 13:04 UTC-4, para poder abranger toda a base de dados.

Para identificar um ataque de DDoS massivo e de grande escala, é necessário observar um aumento significativo no uso de portas diferentes e no tamanho dos pacotes, como resultado disso. Inicialmente, com auxílio do histograma, foram analisados o histórico dos dados e como eles se comportam.

A Figura 1 relaciona a porta destino e a densidade dela em relação às portas utilizadas com o passar do tempo no Timestamp. Quanto mais escura a cor utilizada, maior a quantidade de pacotes dentro daquela porta determinada porta e momento.

Figura 1 – Densidade de Porta de utilização das portas em um período.



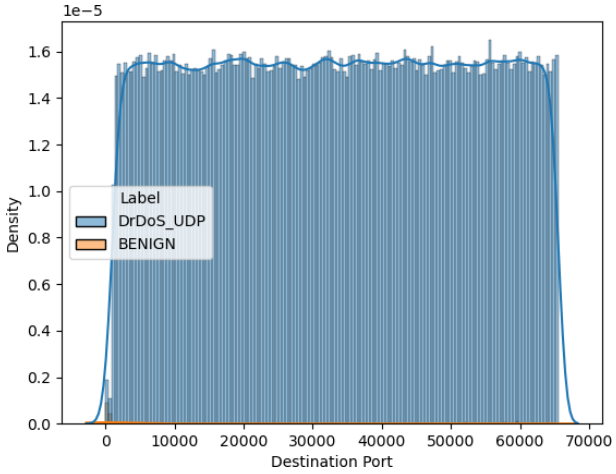
Fonte: Elaborado pelo autor.

Na Figura 1 podemos ver que entre os minutos 12:54 e 12:55, há um aumento da intensidade de utilização das portas, mostrada pela variação de cores. Com base no horário, é possível identificar algum tipo de alteração ou um possível ataque.

Observando um aumento repentino na utilização em um determinado horário, buscou-se compreender a densidade do gráfico, sendo que o destaque principal foi a coluna de destino da porta, evidenciando a densidade das portas e suas variações numéricas. A Figura 2 ilustra essa relação.

Na Figura 2, é apresentado o uso de cada porta em relação a densidade, onde podiam variar entre pouco utilizado e muito utilizado. Um alto uso por parte do DDoS seria uma evi-

Figura 2 – Densidade das utilizações das portas



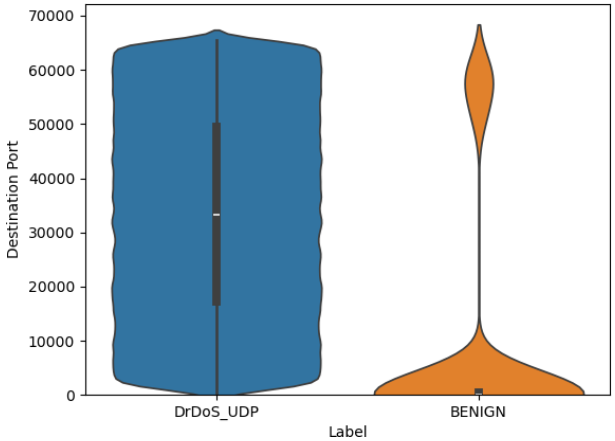
Fonte: Elaborado pelo autor.

dência de maior densidade, embora se isso ocorresse com informações benignas, demonstraria ser algo normal e não necessitaria de análise adicional. Essa figura abrange o horario mostrado anteriormente.

É visível um aumento no uso dessas portas em relação aos dados benignos e DDoS. Os dados relacionados ao DDoS apresentam maior uso em comparação aos dados benignos, indicando que um ataque DDoS UDP pode concentrar-se em uma utilização e sobrecarga maiores dessas portas. Considerando isso, o gráfico de Violino permite comparar a distribuição de uma variável em diferentes categorias. Ele é utilizado para representar a comparação da distribuição de uma variável (ou distribuição de amostra) em diferentes categorias.

Em análises de ataques DDoS, um gráfico de violino pode servir para visualizar a distribuição de várias métricas associadas ao tráfego de rede e sua utilização. A representação da distribuição dos pontos, mostrando a densidade de utilização em cada porta, está apresentada na Figura 3, ilustrando essa relação.

Figura 3 – Distribuição de pontos de Dados para Dados DDoS e Dados Benignos.

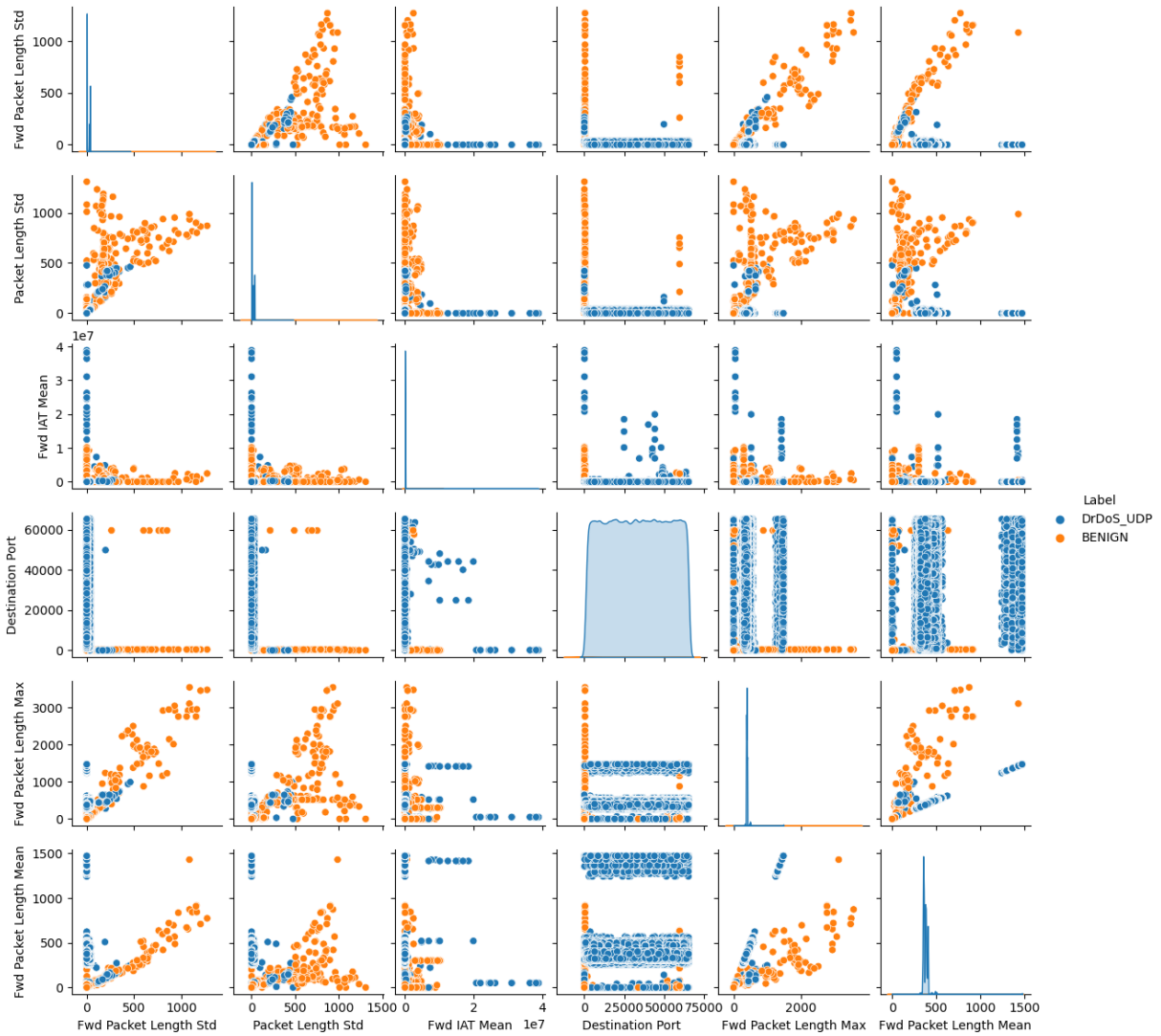


Fonte: Elaborado pelo autor.

Com base na Figura 3, é possível inferir que os usuários que realizam ataques DDoS tendem a distribuir seus ataques em uma ampla gama de portas. Por outro lado, o tráfego benigno tende a se concentrar em portas de menor número, sendo reservadas para serviços de rede comuns. Além disso, a forma da distribuição nos dados benignos é mais estreita e não uniforme, enquanto a forma da distribuição nos dados de DDoS é mais espalhada. Isso poderia ser indicativo dos tipos de ataques realizados, bem como dos tipos de tráfego benignos observados.

Para explorar a relação entre atributos da base de dados, foi utilizado o Gráfico de Relações Pareadas, que possibilita entender como uma variável se comporta em relação à outra. A Figura 4 ilustra essa relação.

Figura 4 – Relações de distribuições bivariadas em um conjunto de dados, dados benignos e de DDoS.



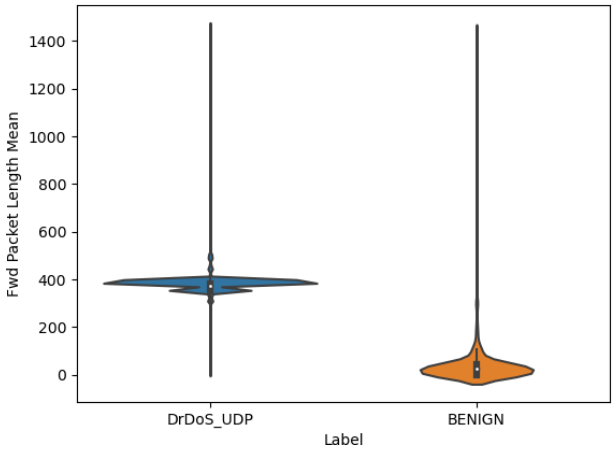
Fonte: Elaborado pelo autor.

Na Figura 4, uma das relações apresentadas, é o comportamento do DDoS, foi o "FWD PACKET LENGTH MEAN", correspondente à média do tamanho dos pacotes de dados encaminhados em uma determinada rede de computadores. Além disso, foi possível identificar

também relações de entre eles também nas seguintes colunas: "Fwd Packet Length Std", "Fwd IAT Mean", "min_seg_size_forward", "Destination Port"e "Protocol", pois as interações entre elas mostrava esse comportamento mencionado.

A Figura 5 mostra como a coluna selecionada está sendo distribuída, permitindo a visualização tanto do tráfego DDoS quanto do tráfego benigno. Ela apresenta uma diferença entre os dois, onde os pacotes benignos tem um tamanho menor (entre 0 a 200) que os de DDoS (de 250 a 450), mostrando assim uma diferença entre eles. Isso sugere uma abordagem potencial para análise e teste.

Figura 5 – Distribuição de Pontos de Dados, do tamanho médio dos pacotes, em relação a Dados Benignos e de DDoS.



Fonte: Elaborado pelo autor.

5.2 Treinamento dos Algoritmos

O treinamento foi realizado utilizado a biblioteca Scikit-learn, que contém os algoritmos do Random Forest, para treinamento da base de dados, após etapa de pre-processamento. Foram realizados 3 experimentos.

5.3 Experimento 1: Identificação de DDoS e tráfego benigno na base de dados completa

O primeiro experimento foi realizado com a base de dados completa. Utilizando a primeira parametrização do algoritmo, foi observado um comportamento relacionado ao overfitting, uma vez que a árvore produziu até 19 níveis - neste caso, o Random Forest continha nós-folha com apenas 2 amostras. O método obteve uma precisão de 100% na classificação de dados de DDoS, mas apenas 98% na classificação de dados benignos.

Ao avaliar o comportamento do algoritmo, observou-se que a redução da quantidade de níveis da árvore produzia comportamento semelhante, com um número de níveis menor. Ficou

decidida a utilização 100 árvores de decisão com no máximo 5 níveis, permitindo interpretação e bons resultados.

Na árvore criada, a distribuição das amostras revela uma disparidade: 99,93% dos dados correspondem a ataques DDoS, enquanto apenas 0,07% são dados classificados como Benignos, representando uma diferença de mais de 1400 vezes entre as duas classes. A Tabela 1 mostra os resultados encontrados do treinamento.

Floresta aleatória	**Precisão**	**Amostras**
BENIGN	98%	531
DrDoS_UDP	100%	783.670
Macro AVG	99%	784.201
Weighted AVG	100%	784.201

Tabela 1 – Métricas para a Floresta Aleatória utilizando toda a base de dados.

Na Tabela 1, é possível indicar que a classificação do DDoS com 100% e das informações benignas com 98%, foi bem sucedida.

5.4 Experimento 2: Identificação de DDoS e tráfego benigno no início dos ataques

Como é possível identificar visualmente quando é um ataque de negação de serviço é iniciado, considerando os gráficos analisados, foi feito um filtro no horário de início do ataque, entre 12:54 e 12:55, e a partir desse horário foi refeito o treinamento para identificá-lo. A Tabela 2 abaixo mostra o treinamento para esta situação. Ele obteve um resultado de 100%, classificando perfeitamente os dados com árvores de até 5 níveis.

Floresta aleatória	**Precisão**	**Amostras**
BENIGN	100%	62;
DrDoS_UDP	100%	5.307
Macro AVG	100%	5.369
Weighted AVG	100%	5.369

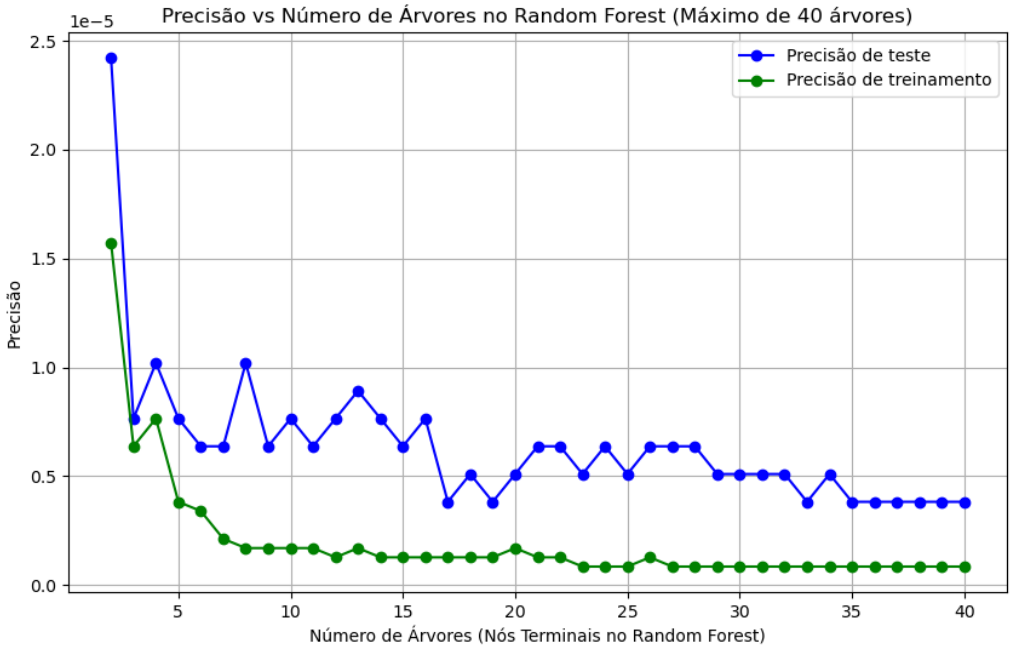
Tabela 2 – Métricas para a Floresta Aleatória com treinamento entre 12:54 e 12:55.

Na Tabela 2, é perceptível que, apesar da escassez de dados relacionados ao DDoS, houve eficácia na classificação e aprendizado sobre o comportamento desses dados, onde o algoritmo Random Forest obteve uma acurácia de 100% na classificação dos dados de DDoS e de 100% na classificação dos dados benignos. A quantidade de informações disponíveis para o DDoS é limitada em comparação com outros conjuntos de dados, porém isso não impediu a identificação eficiente dos dados classificados como DDoS e, especialmente, dos dados benignos.

5.5 Overfitting

O algoritmo do Random Forest, chegou a criar 19 níveis de árvores. Na Figura 6 é possível ter essa visualização de como o modelo vai aprendendo e a precisão vai aumentando, até chegar o momento que as duas retas ficam de iguais de nível de evolução.

Figura 6 – Score vs Número de Árvores no Random Forest (Máximo de 40 árvores).



Fonte: Elaborado pelo autor.

A precisão do modelo é fundamental para avaliar seu desempenho nas classificações. Inicialmente alta, ela gradativamente se estabiliza em comportamentos mais lineares das curvas de aprendizado, indicando a necessidade de interromper o overfitting. O ponto crítico identificado, número 5, marca o início desse equilíbrio, sinalizando o término do overfitting. Nessa etapa, o modelo mantém boa precisão nas classificações sem se adaptar excessivamente aos dados de treinamento.

5.6 Experimento 3: Análise da capacidade de generalização

O presente teste foi criado para verificação do desempenho de treinamento do experimento detalhado na Seção 5.4 em toda a base de dados. Tal teste visou avaliar se o treinamento poderia ser afetado pela distribuição desigual dos dados de DDoS e Benignos, conforme mostrado na tabela 3. O objetivo foi testar o desempenho do algoritmo em um intervalo de tempo diferente, onde os dados benignos e de DDoS estão mais balanceados. Esse intervalo foi es-

colhido entre 12:54 e 12:55, conforme mostrado na figura 1 . A Tabela 3 mostra os resultados obtidos da execução do algoritmo treinado Seção 5.4 em toda a base de dados.

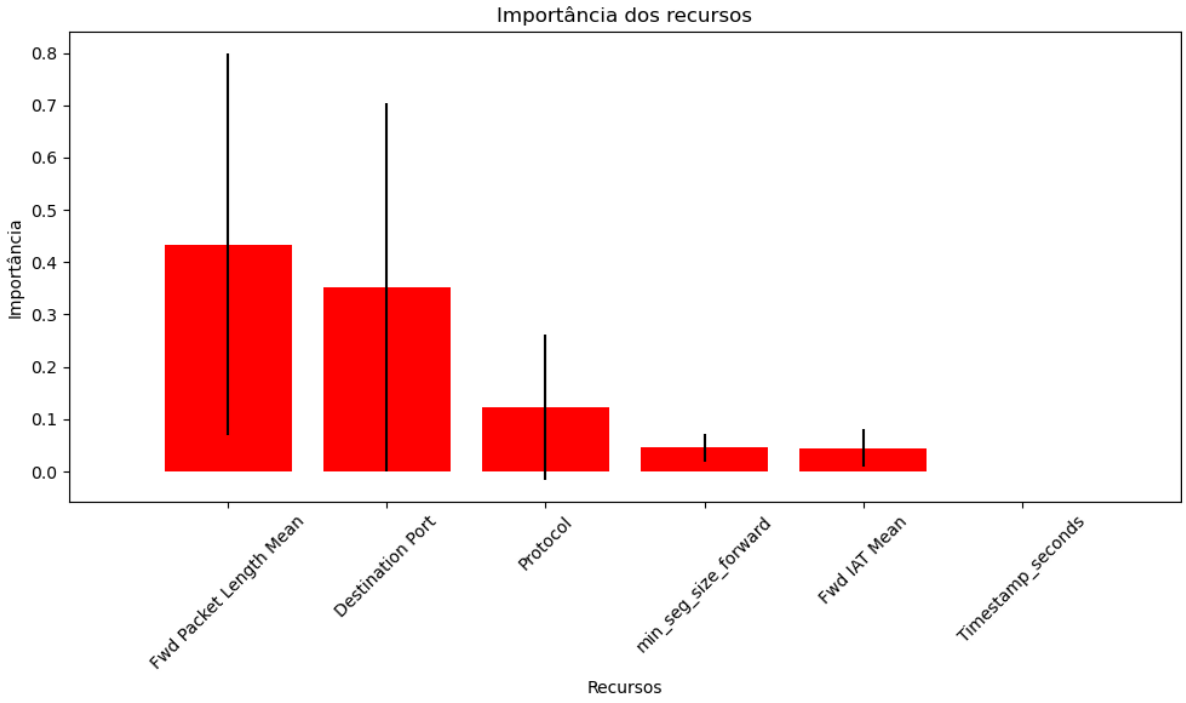
Floresta aleatória	**Precisão**	**Suporte**
BENIGN	83%	531
DrDoS_UDP	100%	783.670
Macro AVG	91%	784.201
Weighted AVG	100%	784.201

Tabela 3 – Métricas para toda a base de dados, com treinamento de informações entre 12:54 e 12:55.

Para o DDoS, é possível ver que ele classificou em 100% dos casos de DDoS, mas para os dados benignos, teve uma taxa de acertos de 83%. Apesar da diferença na quantidade de amostras em relação experimento anterior, é algo que se assemelha à realidade, já que haveria um fluxo menor que o ataque de negação de serviço. Para a média de classificação em geral do algoritmo, ele obteve uma classificação ainda melhor, atingindo 91%.

Por fim, a análise da relevância das características em um modelo de aprendizado de máquina, especificamente no contexto do Random Forest, é essencial. Visualizar os recursos e sua importância é fundamental. A figura seguinte representa essa relação para validar a escolha feita.

Figura 7 – Análise de Importância dos Recursos com Floresta Aleatória.



Fonte: Elaborado pelo autor.

Na figura 7, são exibidos os recursos: “Fwd Packet Length Mean”, “Destination Port”,

“Protocol”, “min_seg_size_forward”, “Fwd IAT Mean” e “Timestamp seconds”. As características “Fwd Packet Length Mean” e “Destination Port” exibem barras mais altas, indicando maior relevância para o modelo, corroborando a análise exploratória e destacando a importância desses atributos.

6 CONCLUSÃO

Neste estudo, investigamos a relação do comportamento do DDoS na base de dados *"DDoS Evaluation Dataset (CIC-DDoS2019)"* (SHARAFALDIN et al., 2019), onde procuramos classificar tráfego DDoS e informação benigna. O resultado apresentado indica que é viável identificar e classificar o tráfego, mesmo em meio a um ataque DDoS do tipo inundação de UDP utilizando o algoritmo Random Forest. Isso possibilita o tráfego de informações benignas durante esses eventos.

A importância desse estudo está na contribuição para a análise exploratória e identificação eficaz do ataque DDoS e do tráfego benigno. Os resultados obtidos podem ser úteis para profissionais de segurança da informação que buscam identificar e lidar com esses tipos de ataques.

Os objetivos foram alcançados, pois conseguimos fazer a análise das informações da base de dados e por meio do Random Forest e da análise exploratória, verificar as principais características apresentadas na base de dados. E, por fim, foram obtidos 83% de classificação de usuários benignos.

Em conclusão, destaca-se a significância da classificação precisa do tráfego DDoS e dos dados benignos na base de dados analisada. Os resultados obtidos são esperados para contribuir para análises futuras, assegurando a continuidade do tráfego normal para indivíduos que possuem informações benignas e não estão vinculados ao ataque. Essa classificação pode se fazer eficaz e crucial para manter a integridade das operações durante eventos de ataques DDoS.

O código-fonte do trabalho está publicamente disponível em <https://github.com/davijls9/-algoritmo-Random-Forest-para-identifica-DDoS-UDP> .

Referências

AL-DUNAINAWI, Yousif; AL-KASEEM, Bilal R.; AL-RAWESHIDY, Hamed S. Optimized artificial intelligence model for ddos detection in sdn environment. **IEEE Access**, v. 11, p. 106733–106756, 2023. Disponível em: <https://ieeexplore.ieee.org/document/9567876>. Acesso em: 16 de Dez. 2023.

CHEN, Liguo et al. Detection of dns ddos attacks with random forest algorithm on spark. p. 1–4, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1877050918311426?ref=pdf_download&fr=RR-2&rr=803a541e28327523>. Acesso em: 8 de set. 2023.

CORSINI, Andrea; YANG, Shanchieh Jay; APRUZZESE, Giovanni. On the evaluation of sequential machine learning for network intrusion detection. p. 1–10, 2021. Disponível em: <https://dl.acm.org/doi/10.1145/3465481.3470065>. Acesso em: 9 de abr. 2023.

CYBERSECURITY, Canadian Institute for. Ddos evaluation dataset (cic-ddos2019). 2019. Disponível em: <https://www.unb.ca/cic/datasets/ddos-2019.html>. Acesso em: 6 de set. 2023.

DAS, Rammanohar; SANDHANE, Raghav. Artificial intelligence in cyber security. doi:10.1088/1742-6596/1964/4/042072, 21 pages, p. 1–21, 2021. Disponível em: <https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/pdf>. Acesso em: 19 de mar. 2023.

FOSIć, Igor et al. Anomaly detection in netflow network traffic using supervised machine learning algorithms. Volume 33, June 2023, 100466, 1 pages, p. 1–1, 2023. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S2452414X23000390>. Acesso em: 2 de mai. 2023.

GARCíA, S.; GRILL, J. Stiborek M.; ZUNINO, A. An empirical comparison of botnet detection methods. Canada, 2014. Disponível em: <http://dx.doi.org/10.1016/j.cose.2014.05.011>. Acesso em: 1 de dez. 2023.

HOU, Jiangpan et al. Machine learning based ddos detection through. doi:10.1088/1742-6596/1964/4/042072, 6 pages, p. 1–6, 2018. Disponível em: <https://ieeexplore.ieee.org/document/8599738>. Acesso em: 24 de mar. 2023.

INSIGHT-LAB. Por que o python é a linguagem mais adotada na área de data science. 2023. Disponível em: <DisponÃ■velem:\url{https://insightlab.ufc.br/por-que-o-python-e-a-linguagem-mais-adotada-na-area-de-data-science/}.Acessoem: 13dedez.20>.

IX.BR. Em nova marca recorde, IX.br ultrapassa os 31 tbit/s de pico de troca de tráfego de internet. In: COMITê GESTOR DA INTERNET NO BRASIL – CGI.BR. [S.l.], 2023. Disponível em: <https://ix.br/noticia/releases/em-nova-marca-recorde-ix-br-ultrapassa-os-31-tbit-s-de-pico-de-troca-de-trafego-internet>. Acesso em: 29 de nov. 2023.

KEMP, Clifford; CALVERT, Chad; KHOSHGOFTAAR, Taghi M. Detecting slow application-layer dos attacks with pca. DOI: 10.1109/IRI51335.2021.00030, 8 pages, p. 1–8, 2021. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S2452414X23000390>. Acesso em: 7 de abr. 2023.

LAI, Yingxu; ZHANG, 1 Jingwen; LIU, Zenghui. Industrial anomaly detection and attack classification method based on convolutional neural network. Volume 2019, Article ID 8124254,

11 pages, p. 1–11, 2019. Disponível em: <https://downloads.hindawi.com/journals/scn/2019/8124254.pdf>. Acesso em: 19 de fev. 2023.

MEKALA, Srinivas; DASARI, Kishore Babu. Netbios ddos attacks detection with machine learning classification algorithms. DOI: 10.1109/InCACCT57535.2023.10141815, p. 1–4, 2023. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10141815>. Acesso em: 7 de set. 2023.

OKADA, Hugo Kenji Rodrigues et al. Árvores de decisão: estruturas de dados. 2023. Disponível em: <https://doi.org/10.33448/rsd-v8i11.1473>. Acesso em: 18 de Novembro de 2023.

RAJA, Mr.S.S.Vasantha et al. Prediction of cyber attacks using machine learning technique. ISSN:2320-2882, p. 40–51, 2022. Disponível em: <https://ijcrt.org/papers/IJCRTS020006.pdf>. Acesso em: 14 de fev. 2023.

SHARAFALDIN, Iman; LASHKARI, Arash Habibi; GHORBANI, Ali A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. Canada, 2018. Disponível em: <https://pdfs.semanticscholar.org/2342/9b5be933e16e6988da9a322ad95dfdc8c4b0.pdf>. Acesso em: 1 de dez. 2023.

SHARAFALDIN, Iman et al. Developing realistic distributed denial of service (ddos) attack dataset and taxonomy. 2019. Disponível em: <https://www.unb.ca/cic/datasets/ddos-2019.html>. Acesso em: 23 de Out. 2023.

SILVA, Luiza Maria Oliveira da. Uma aplicação de Árvores de decisão, redes neurais e knn para a identificação de modelos arma não-sazonais e sazonais. 2005. Disponível em: <https://doi.org/10.17771/PUCRio.acad.7587>. Acesso em: 18 de nov. 2023.

SILVA, Nícolas Rocha e; SALLES, Ronaldo Moreira. Métricas para detecção de ataques DDoS. 4° Trimestre de 2015, 21 pages, p. 1–21, 2015. Disponível em: <https://rmct.ime.eb.br/arquivos/RMCT_4_tri_2015/RMCT_228_E8A_14.pdf>. Acesso em: 8 de mar. 2023.

WATKINS, John; TUMMALA, Murali; MCEACHEN, John. A machine learning approach to network security classification utilizing netflow data. DOI: 10.1109/ICSPCS53099.2021.9660294, 10 pages, p. 1–21, 2021. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S2452414X23000390>. Acesso em: 21 de abr. 2023.

YOACHIMIK, Omer; PACHECO, Jorge. Relatório sobre ameaças ddos no t1 de 2023. 2023. Disponível em: <https://blog.cloudflare.com/pt-br/ddos-threat-report-2023-q1-pt-br/>. Acesso em: 13 de dez. 2023.