2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS) | 979-8-3503-8306-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISAS60782.2023.10391487

Detection of Distributed Denial-of-Service (DDoS) Attack with Hyperparameter Tuning Based on Machine Learning Approach

Wan Nurulsafawati Wan Manan
Faculty of Computing
Universiti Malaysia Pahang
Al-Sultan Abdullah
26600 Pekan, Pahang, Malaysia
safawati@umpsa.edu.my

Choo Yong Han
Faculty of Computing
Universiti Malaysia Pahang
Al-Sultan Abdullah
26600 Pekan, Pahang, Malaysia
yhchoo017@gmail.com

Abstract— **Distributed Denial-of-Service (DDoS) attack is a malicious cyber-attack which targets availability element in CIA triad and to disrupt the availability of network services of a target by performing a huge malicious traffic flood. To conduct the study, a standard benchmark dataset DDoS Attack SDN Dataset is applied. EDA and Data Pre-processing are performed to ensure a clean dataset is produced for obtaining an accurate and meaningful detection performance results. Hyperparameter tuning is performed to enhance the detection performance of the models. It is proposed that DNN shows the promising results as it has shown 99.84% accuracy to detect DDoS attack after performing hyperparameter tuning. It is observed that hyperparameter tuning has improved and increased most of the performance results of DNN and DT, with increment 4.84% in DT while 0.97% in DNN. Besides, the detection results have been increased and their false detection has been reduced. This study could help to reduce the dwell time of DDoS attack, increase the Mean Time To Contain (MTTC) and avoid alarm fatigue.**

Keywords—DDoS attack, Machine Learning, Hyperparameter Tuning, Detection, Availability, GridSearchCV

I. INTRODUCTION

Distributed Denial-of-Service (DDoS) attack is a sophisticated and dangerous malicious web-based attack which targets availability element from CIA traid by refusing the legitimate users to enter the services and send the huge malicious packets to disrupt the services. The targeted services or systems will experience slower performance, crash and being compelled to shut down. There are several motivations for attackers to launch this attack such as ruin the reputation of a company or organization and being a hacktivist to protest to show their disappointment or opinions on local or global issues.

To launch the DDoS attack, the attacker will recruit an army of botnets or zombies by spreading the sophisticated malware and infect the targeted devices to turn them into botnets. Next, these botnets will connect to Control and Command (CnC) server which belongs to attacker and ready to receive the instructions from attacker. After that, the botnets will follow the instructions from attacker to launch a well-planned distributed attack by sending huge malicious requests after the attacker send the instructions to CnC server. For instance, Mirai Botnet which launched by attacker has caused almost 900 thousand users of Deutsche Telekom Internet Service Provider (ISP) were unable to access to Internet as their routers being attacked by Mirai botnet[1].

DDoS attack becomes a main concern when it shows the high spiking of numbers of launching the DDoS attack from year to year. Kaspersky stated that DDoS has showed a significant increase in the third quarter of 2022, which was 47.87% compared to third quarter of 2021[2]. Moreover, Microsoft observed attacks over TCP-based method was the most frequent attack form launched in 2022, which were 63% compared to other protocols such as UDP-based attacks which were 22% and packet anomaly attacks which were 15%. Most of the attacks launched are less than one hour which is a shorter duration attack to save the device resources[3]. Cloudflare also found that most attacks peaked between 50 and 70 million requests per second (rps) with the biggest attack exceeding 71 million rps in February 2023 which is the biggest HTTP DDoS assault over reported[4]. This has caused a huge damage to the national economy and society in recent years [5]. For instance, Anonymous Sudan hacker group has conducted DDoS attack to shut down nine Danish hospital's websites for several hours in reprisal for Quran-burning activists and politicians who had recently done so in Denmark to express their discontent in February 2023[6]. This has caused disruption to work properly in hospital sector which was dealing with online activities such as inquiries. On the other hand, IT Army of Ukraine, a pro-Ukraine hacktivist group has admitted for launching the DDoS attack to shutdown VTB Bank in Russia in December 2022 to disrupt the payment processing and ruin the bank's reputation[7].

A study conducted by [11] on the detection of DDoS attack suggested that Random Forest algorithm is the best machine learning model which shows promising results where 99.88% accuracy, 99.88% precision, 100.00% recall and 0.05% false alarm rate compared to other proposed supervised machine learning algorithms which are Logistic Regression, K-Nearest Neighbors, Gaussian Naïve Bayes, Decision Tree, SVM-Sigmoid, SVMPolynomial and SVM-RBF.

Next, a study analysis conducted by performance of three machine learning algorithms which are Artificial Neural Network

979-8-3503-8306-5/23/$31.00 ©2023 IEEE