BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Banyaknya serangan yang terjadi pada sebuah sistem elektronik dapat mengganggu kinerja sebuah industri atau bisnis. Salah satu serangan yang populer adalah serangan pada sisi jaringan dengan menguras habis bandwith atau resources yang dimiliki atau dengan kata lain serangan DDoS (*Distributed Denial of Service*). DDoS disebut sebagai senjata andalan hacker karena telah terbuki menjadi ancaman permanen bagi pengguna, organisasi dan infrastruktur di internet.

Di sisi lain, serangan jaringan merupakan resiko untuk integritas, kerahasiaan dan ketersediaan sumber daya yang disediakan oleh organisasi atau dapat kita sebut dengan CIA (*Confidentiallity, Integrity, Availability*). Salah satu upaya yang dilakukan untuk menangani serangan ini adalah dengan mendeteksi serangan DDoS menggunakan *Machine Learning* dengan tingkat akurasi yang cukup tinggi.

Machine Learning atau pembelajaran mesin merupakan sebuah teknik bagaimana cara komputer mampu belajar seperti manusia dengan mengenal data yang diberikan. Upaya dalam mendeteksi sebuah serangan DDoS menggunakan *Machine Learning* merupakan kegiatan proaktif atau kegiatan yang membuat kita sebagai *security engineer, system administrator* atau orang yang bertanggung jawab dalam hal ini selangkah lebih maju daripada *threat actor* sehingga sistem kita dapat membaca bahwa terdapat anomali yang kemudian pada *endpoint* dapat dilakukan *blocking* atau singkatnya sebagai upaya preventif. Tentunya dalam mendeteksi anomali serangan juga membutuhkan algoritme atau sebuah metode yang tepat untuk memprediksi, mendeteksi dan mengklasifikasikan apakah termasuk serangan DDoS atau bukan. Dengan melakukan komparasi pada beberapa model *Machine Learning* yang ada sehingga dapat ditemukanlah metode yang cocok dengan dataset yang ada sehingga menghasilkan nilai akurasi yang tinggi untuk melakukan deteksi dan klasifikasi pada masalah yang ada.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang yang dijelaskan sebelumnya, dapat dirumuskan sebuah permasalahan sebagai berikut :

1. Bagaimana cara mendeteksi dan klasifikasi serangan DDoS menggunakan Machine Learning?
2. Berapa tingkat peforma dari algoritme KNN, Naïve Bayes, *Stochastic Gradient Descent* dan XGBoost dengan parameter akurasi, recall dan F1-Score.

1.3 Batasan Masalah

Untuk mempersempit pembahasan pada skripsi ini, maka dibuat batasan-batasan sebagai berikut:

1. Dataset yang digunakan adalah data yang langsung berasal dari sistem pada CV. Hardi Junior dan dilakukan *dump* pada tanggal 29 November 2021
2. Bahasa pemrograman dan software yang digunakan dalam skripsi ini adalah *Python*, *Google Colab* serta beberapa library pendukung seperti *pandas, sklearn, matplotlib, seaborn, numpy* dan *keras*
3. Melakukan deteksi dan klasifikasi dengan menggunakan algoritme KNN, Naïve Baiyes, *Stochastic Gradient Descent* dan XGBoost

1.4 Tujuan Penelitian

Tujuan yang ingin diraih dalam pembuatan laporan skripsi ini adalah:

1. Mengetahui algoritme mana yang lebih efektif dan cocok digunakan untuk mendeteksi serangan DDoS pada CV. Hardi Junior.