BAB I
PENDAHULUAN

1.1. Pendahuluan

Dunia maya negara-negara dan negara-negara di seluruh dunia telah menyaksikan sejumlah besar insiden siber dalam beberapa waktu terakhir. Beberapa insiden siber ini dilakukan dengan menggunakan bypass operasional yang dapat dideteksi seperti non-aplikasi pembaruan keamanan dan peningkatan. Perusahaan perangkat lunak dan perangkat keras secara berkala merilis pembaruan dan peningkatan berkala sebagai cara untuk membuat produk mereka sangat mudah. Namun, pembaruan keamanan hanya dirilis untuk kerentanan yang diidentifikasi dalam produk perangkat lunak atau perangkat keras. Ketika kerentanan semacam itu tidak terdeteksi cukup awal, hal itu dapat menimbulkan masalah keamanan serius bagi negara mana pun. Ketika tidak ada informasi sebelumnya tersedia untuk kerentanan tertentu, dan kerentanan tersebut dieksploitasi oleh pengguna jahat, eksploitasi nol hari tidak bisa dihindari.

Data dari BSSN Tahun 2018 menunjukan bahwa sebanyak 2.238.776 serangan siber dilakukan, *Denial of Service (DoS), Stuxnet, Ramnit, Polymorphic Worms, Flame, Ransomware, Malware,* dan sejenisnya adalah contoh ancaman yang memicu banyak insiden serangan siber di dunia maya [1]. Sejalan dengan semakin banyak serangan yang terjadi, Salah satu serangan yang dilakukan adalah serangan DOS. Serangan DOS adalah jenis serangan di mana peretas membuat komputasi atau sumber daya memori terlalu sibuk atau terlalu penuh untuk melayani permintaan jaringan yang sah dan karenanya menolak akses pengguna ke mesin [2].

Pengembangan serangan DOS yaitu dengan mendistribusikan serangan DOS tersebut atau disebut dengan *Distibuted Denial of Service (DDoS)*. Adapun macam-macam serangan *Distibuted Denial of Service (DDoS)* yang sering digunakan para hacker untuk menyerang diantaranya *SYN-Flooding, SMURF Attack, UDP-Flooding, ICMP-Flooding, UDP-Attack, DNS-Flooding* dan sebagainya.

Berdasarkan serangan DDoS tersebut, ada banyak teknik yang bisa digunakan dalam mendeteksi serangan DDoS, teknik tersebut diantaranya yaitu dengan menggunakan algoritma *Machine Learning*, didalam *Machine Learning* ada banyak algoritma yang bias digunakan, diantaranya; *Supervised Learning, Unsupervised Learning,* dan *Semi-Supervised Learning*.

Aplikasi algoritma *Machine Learning* tersebar dalam berbagai macam. Salah satu pengaplikasian yang paling signifikan adalah Klasifikasi. Ada beberapa teknik klasifikasi *Machine Learning* diantaranya seperti klasifikasi dengan menggunakan algoritma *Bayesian Network, Support Vector Machines, Decision Tree (ID3, C4.5, C5.0, J48), OneR, dan K-Nearest Neighbor Classifier*. Masing-masing teknik ini mempertimbangkan aspek-aspek berbeda dari *dataset* dan memberikan klasifikasi yang akurat.

Mengacu pada metode yang dijabarkan diatas, maka penelitian ini akan menggunakan metode yang ada pada beberapa algoritma *Machine Learning* Penelitian ini menggunakan *dataset* jaringan DDoS CICDDoS2019 yang ditulis oleh Canadian Institute for Cybersecurity [3]. Pada penelitian ini juga bertujuan untuk memberikan solusi untuk serangan *Distributed Denial of Service (DDoS)* dengan klasifikasikan hasil dari *dataset* tersebut menggunakan algoritma *Machine Learning* yang diantaranya *Decision Tree, K-NN, Bayesian Network* dan *OneR*.

1.2. Rumusan Masalah

Rumusan masalah yang akan diteliti adalah sebagai berikut:

a. Bagaimana cara mengklasifikasikan data yang ada pada *Dataset* serangan DDoS CICDDoS2019 menggunakan algoritma *Machine Learning* yang diantaranya *Decision Tree, K-NN, Bayesian Network* dan *OneR*.
b. Bagaimana hasil dari perbandingan beberapa hasil klasifikasi dari data serangan DDoS CICDDoS2019 menggunakan metode yang terdapat pada algoritma *Machine Learning* yang diantaranya *Decision Tree, K-NN, Bayesian Network* dan *OneR*.

1.3. Batasan Penelitian

Batasan penelitian pada penelitian ini adalah sebagai berikut:

a. Dataset serangan DDoS yang digunakan yaitu CICDDoS2019 yang ditulis oleh Canadian Institute for Cybersecurity.
b. Penelitian ini menggunakan serangan-serangan pada DDoS yang diantaranya *TCP-Attack (SYN-Flood) dan UDP-Attack (NTP)*.
c. Algoritma yang digunakan dalam mengklasifikasikan serangan DDoS sendiri dengan menggunakan algoritma *Machine Learning* yang diantaranya *Decision Tree, K-NN, Bayesian Network* dan *OneR*.
d. Program data mining yang digunakan untuk mengklasifikasikan data serangan tersebut menggunakan WEKA (Waikato Environment for Knowledge Analysis).

1.4. Tujuan Penelitian

Tujuan penelitian ini yaitu:

a. Mendeteksi hasil klasifikasi dari serangan-serangan pada DDoS menggunakan algoritma algoritma *Machine Learning* yang diantaranya *Decision Tree, K-NN, Bayesian Network* dan *OneR*.
b. Menganalisa hasil klasifikasi dari serangan-serangan pada DDoS yang diantaranya *TCP-Attack (SYN-Flood) dan UDP-Attack (NTP).*
c. Melakukan perbandingan terhadap hasil klasifikasi dan menyimpulkan hasil analisa terhadap hasil klasifikasi tersebut dengan menggunakan metode yang terdapat pada algoritma *Machine Learning* yang diantaranya *Decision Tree, K-NN, Bayesian Network* dan *OneR*.

1.5. Manfaat Penelitian

Manfaat penelitian ini yaitu:

a. Mengetahui bagaimana cara mengklasifikasikan data yang ada pada *dataset* serangan DDoS CICDDoS2019 menggunakan algoritma *Machine Learning* yang diantaranya *Decision Tree, K-NN, Bayesian Network* dan *OneR*
b. Mengetahui bagaimana hasil dari perbandingan beberapa hasil klasifikasi data serangan DDoS CICDDoS2019 menggunakan metode yang terdapat pada algoritma *Machine Learning* yang diantaranya *Decision Tree, K-NN, Bayesian Network* dan *OneR*

1.6. Sistematika Penulisan

Sistematika penulisan pada tesis ini dibagi atas beberapa bab serta masing-masing bab terbagi menjadi beberapa sub bab. Berikut adalah gambaran dari tiap bab:

a. **BAB I PENDAHULUAN**

   Bab ini tercantum latar belakang, perumusan masalah, ruang lingkup penelitian, tujuan dan manfaat penelitian dan sistematika penulisan.

b. **BAB II LANDASAN TEORI**

   Pada bab ini memuat tentang teori-teori yang mendukung penelitian yang dilakukan.

c. **BAB III METODE PENELITIAN**

   Dalam bab ini berisi metode mengklasifikasi dan menganalisa serta membandingan dari metode tersebut.

d. **BAB IV HASIL DAN PEMBAHASAN**

   Bab ini memberikan hasil dari proses klasifikasi terhadap data serangan DDoS yang dilakukan dan menunjukan perbandingan dari beberapa metode klasifikasi yang digunakan.

e. **BAB V SIMPULAN DAN SARAN**

   Bab ini berisikan kesimpulan dari hasil klasifikasi dan perbandingan dari beberapa metode yang digunakan. Pada bab ini juga diberikan saran guna perkembangan penelitian lebih lanjut kedepannya.

f. **DAFTAR PUSTAKA**

g. **LAMPIRAN**