BAB V
SIMPULAN DAN SARAN

5.1. Simpulan

Berdasarkan penelitian yang telah dilakukan, simpulan yang dapat dipaparkan diantaranya sebagai berikut:

a. Pada penelitian ini *dataset* DDoS yang digunakan yaitu *dataset* jaringan DDoS CICDDoS2019 yang ditulis oleh Canadian Institute for Cybersecurity.
b. Pada penelitian ini menggunakan 2 jenis serangan DDoS, serangan tersebut adalah serangan serangan SYN Flood (Berdasarkan Serangan TCP-Serangan Exploitasi) dan serangan NTP (Berdasarkan Serangan UDP-Serangan Refleksi).
c. Analisan dan proses klasifikasi data tersebut menggunakan program *data mining* WEKA (Waikato Environment for Knowledge Analysis).
d. Pada kedua serangan DDoS tersebut menggunakan *sampel* sebanyak 10% dari *dataset* di tiap serangan DDoS. Adapun total *dataset* DDoS pada serangan SYN sebanyak 1.582.682 *record* data, pada *dataset* DDoS pada serangan NTP sebanyak 1.217.008 *record* data.
e. Pada kedua serangan DDoS tersebut terdapat 88 atribut dimana semua atribut tersebut digunakan dalam pengolahan data serta pemilihan salah satu atribut "Label" yang digunakan pada proses klasifikasi.
f. Proses klasifikasi dan perbandingan hasil klasifikasi menggunakan algoritma diantaranya *Bayesian Network, IBK(K-NN), OneR,* dan *Decision Tree (J48)*.
g. Pada serangan SYN berdasarkan perhitungan *Sensitivity, Specificity* , *Accuracy* dan *F-measure* pada serangan SYN, nilai tertinggi (*Accuracy*) dicapai pada algoritma *Decision Tree (J48)* dengan nilai 0,999955772. Untuk nilai tertinggi (*Specificity*) dicapai pada algoritma *OneR,* dan *K-NN(Ibk)* yang juga mendapatkan nilai 1,0. Untuk nilai tertinggi (*Sensitivity*) dicapai pada algoritma *BayesNet* dengan nilai 0,999987357. Untuk nilai tertinggi (*F-measure*) dicapai pada algoritma *OneR,* dan *K-NN(Ibk)* dengan nilai keduanya 0,999977882.
h. Pada serangan NTP berdasarkan perhitungan *Sensitivity, Specificity* , *Accuracy* dan *F-measure* pada serangan NTP, nilai tertinggi (*Accuracy*) dicapai pada algoritma *Decision Tree (J48*) dengan nilai 0,999917831. Untuk nilai tertinggi

(*Specificity*) dicapai pada algoritma *OneR* dan *K-NN (Ibk)* yang mendapatkan nilai 1,0. Untuk nilai tertinggi (*Sensitivity*) dicapai pada algoritma *BayesNet* dengan nilai 1,0. Untuk nilai tertinggi (*F-measure*) dicapai pada algoritma *Decision Tree (J48)* dengan nilai 0,999778112.

5.2. Saran

Berdasarkan penelitian yang telah dilakukan, terdapat saran yang dapat dilakukan guna perkembangan penelitian ini kedepannya. Saran tersebut diantaranya:

a. Kedepannya penelitian dapat dilakukan kembali dengan menggunakan jenis serangan lain seperti UDPLag, TFTP, UDP, SSDP, SMNP, dan jenis serangan lainnya yang ada pada *dataset* serangan jaringan DDoS CICDDoS2019 atau menggunakan *dataset* DDoS yang terbaru.
b. Kedepannya penelitian dapat dilakukan kembali dengan menggunakan algoritma untuk klasifikasi yang lain seperti *SVM, ZeroR*, dan algoritma lainnya untuk melihat perbedaan hasil klasifikasinya.
c. Kedepannya penelitian juga dapat dilakukan kembali dengan menggunakan program *data mining* yang lainnya seperti *RapidMiner, AIToolkit, Orange* dan sebagainya.