

BAB 6 PENUTUP

Bagian ini memuat kesimpulan dan saran terhadap skripsi. Kesimpulan dan saran disajikan secara terpisah, dengan penjelasan sebagai berikut:

6.1 Kesimpulan

Berdasarkan pada hasil pengujian, yang diperoleh mengenai proses klasifikasi pada beberapa metode classifier *Naive Bayes*, *SVM Linear*, *SVM Polynomial*, dan *SVM Sigmoid* serta dari pembahasan yang telah dilakukan, maka dapat disimpulkan bahwa:

1. Tahapan klasifikasi serangan menggunakan metode *behavior based* membutuhkan sebuah dataset dan metode. Dengan melakukan perbandingan pola atau aktivitas yang ada pada sebuah data, kemudian dilakukan klasifikasi dengan sebuah metode dan menghasilkan sebuah model. Dari model yang sudah dibangun tersebut diuji dengan data *testing* menghasilkan sebuah *output* untuk melihat akurasi apakah sebuah *traffic* yang ada dapat dikategorikan sebagai intrusi atau bukan.
2. Mekanisme pengolahan dataset ISCX 2012 dilakukan dalam beberapa tahap yaitu dataset ISCX dilakukan *preprocess* dengan mengubah format *xml* menjadi *csv*, dikarenakan format *csv* memiliki tingkat komparabilitas tinggi dan didukung dalam program pengolahan data. Kemudian dilakukan konversi data dari *string* menjadi *integer*, selanjutnya menghilangkan beberapa fitur untuk proses klasifikasi, hingga data siap dimasukkan dalam *classifier*.
3. Fitur yang digunakan dalam proses klasifikasi yaitu *totalSourceBytes*, *totalDestinationBytes*, *totalDestinationPacket*, *totalSourcePacket*, *direction*, *Source TCPFlagsDescription*, *Destination TCPFlagsDescription*, *protocolName*, *sourcePort*, *Destination*, *destinationPort*, *startDateTime*, dan *stopDateTime*. Pemilihan fitur ini bertujuan supaya proses klasifikasi menghasilkan prediksi lebih akurat dengan menghilangkan beberapa fitur yang tidak relevan.
4. Performa yang dihasilkan dari *confusion matrix* pada masing-masing *classifier Naive Bayes*, *SVM Linear*, *SVM Polynomial*, dan *SVM Sigmoid* menghasilkan persentase akurasi berturut-turut sebesar 85,055%, 99,995%, 99,999% dan 99,995%.
5. Performa kinerja klasifikasi yang dihasilkan dari kurva ROC pada *classifier Naive Bayes* yaitu baik, *SVM Linear* lemah, *SVM Polynomial* sangat lemah, dan *SVM Sigmoid* lemah. Sedangkan jika dilihat dari kurva ROC dengan *cross-validation* menunjukkan bahwa *classifier Naive Bayes* yaitu lemah dengan nilai AUC 0,5, *SVM Linear* baik dengan nilai AUC 0,75, *SVM Polynomial* sangat lemah dengan nilai AUC 0,33 dan *SVM Sigmoid* lemah dengan nilai AUC 0,5.

6.2 Saran

Untuk meningkatkan nilai akurasi dari sebuah metode dapat dilakukan dengan beberapa teknik diantaranya teknik *bagging* dan *boosting*. Dalam penelitian ini menggunakan teknik *random sampling* dan belum menggunakan kedua teknik tersebut, karena penelitian ini hanya terbatas pada perbandingan metode *Naive Bayes*, *SVM Linear*, *SVM Polynomial* dan *SVM Sigmoid*. Penelitian ini juga menggunakan data dari ISCX *testbed* 14 Juni 2012 saja. Untuk itu diharapkan pada penelitian selanjutnya dapat digunakan teknik *bagging* maupun *boosting* untuk peningkatan akurasi serta menggunakan dataset ISCX dari *testbed* yang lain yaitu *testbed* ISCX pada tanggal 11-17 Juni.