DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PENGESAHAN iii
HALAMAN MOTTO v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR x
DAFTAR TABEL xii
INTISARI xiii
ABSTRACT xiv
BAB I PENDAHULUAN 1
1.1. Latar belakang 1
1.2. Rumusan masalah 3
1.3. Batasan masalah 3
1.4. Tujuan penelitian 3
1.5. Manfaat penelitian 4
BAB II TINJAUAN PUSTAKA 5
BAB III DASAR TEORI 11
3.1. *Intrusion Detection System* 11
3.2. *Snort* 12
3.3. Dataset 14
3.4. *Machine Learning* 17
3.4.1. *Decision Tree* 18
3.4.2. *Support Vector Machine* 18
3.4.3. *Adapative Boosting* 19
3.4.4. *Extreme Gradient Boosting* 20
3.5. Evaluasi dan Analisis 21
BAB IV METODE PENELITIAN 23
4.1. Alat dan Bahan 23
4.2. Deskripsi Umum Penelitian 23
4.3. Tahapan Penelitian 24
4.4. Perancangan *Dataset* 25
4.4.1. Akuisisi data prioritas 25
4.4.2. Pra-pemrosesan data 27
4.5. Rancangan *Machine Learning* 28
4.5.1. *Decision Tree* 28

4.5.2. *Support Vector Machine* 29
4.5.3. *AdaBoost* 30
4.5.4. *XGBoost* 31
4.5.5. Skenario pelatihan dan pengujian 32
4.6. Rancangan Analisis dan Evaluasi 32

BAB V IMPLEMENTASI **34**

5.1. Konfigurasi *Snort* dan Akuisisi Data Prioritas 34
5.1.1. Konfigurasi variabel pada jaringan 34
5.1.2. Konfigurasi *registered rules* 35
5.1.3. Akuisisi data prioritas 36
5.2. Pra-pemrosesan 38
5.2.1. *Cleaning* dan pemetaan data 38
5.2.2. *One-hot-encoding dan* pemilihan sampel 47
5.3. Implementasi Algoritme *Machine Learning* 50
5.3.1. Pencarian model c*lassifier* 51
5.3.2. *Training* c*lassifier* 53
5.3.3. Klasifikasi data 53
5.3.4. Skor evaluasi 54

BAB VI HASIL DAN PEMBAHASAN **63**

6.1. Hasil Pencarian Nilai Parameter Terbaik 63
6.2. Hasil Klasifikasi Data *Training* dan Data *Testing* 65
6.3. *Confusion Matrix* Hasil Klasifikasi Data *Testing* 66
6.4. Hasil Evaluasi Klasifikasi Data *Testing* 69
6.5. Hasil Evaluasi Klasifikasi Alarm *False Positive* 72

BAB VII PENUTUP **73**

7.1. Kesimpulan 73
7.2. Saran 73

DAFTAR PUSTAKA **74**

DAFTAR GAMBAR

Gambar 3.1 Contoh penulisan aturan *Snort* 12
Gambar 3.2 Paket data jaringan ISCXIDS2012 tanggal 13 Juni 16
Gambar 3.3 *Labeled data flow* ISCXIDS2012 tanggal 13 Juni 16
Gambar 3.4 Respons *Decision Tree* untuk *direct mailing* 18
Gambar 3.5 *Hyperplane* antar kelas 19
Gambar 3.6 *Confusion matrix* untuk klasifikasi *multiclass* 22
Gambar 3.7 Diagram perbandingan performa metode pengklasifikasi dalam hal akurasi, presisi, dan *recall* 22
Gambar 4.1 Diagram alur gambaran umum penelitian 24
Gambar 4.2 Diagram alur perancangan *dataset* 25
Gambar 4.3 Arsitektur Snort 26
Gambar 5.1 Konfigurasi variabel jaringan 34
Gambar 5.2 Arsitektur jaringan testbed ISCXIDS2012 35
Gambar 5.3 Konfigurasi *rules Snort* 35
Gambar 5.4 Contoh perintah untuk mengeksekusi *Snort* 36
Gambar 5.5 Perintah eksekusi *Snort* pada sistem 37
Gambar 5.6 Proses deteksi dan pelabelan prioritas serangan dengan *Snort* 37
Gambar 5.7 Peringatan yang dihasilkan *Snort* 38
Gambar 5.8 *Method* untuk mengonversi *labeled flow dataset* ke dalam *dataframe* 39
Gambar 5.9 *Dataframe* flowdf13 40
Gambar 5.10 Hasil pengubahan tipe data dalam *Dataframe* flowdf13 40
Gambar 5.11 *Method* untuk mengonversi *output Snort* ke dalam *dataframe* 41
Gambar 5.12 Tampilan isi *Dataframe* snortdf13 42
Gambar 5.13 Format asli penulisan kolom *'protocolName'* pada *labeled flow dataset* dan *output Snort* 43
Gambar 5.14 Pengisian data kosong 43
Gambar 5.15 Pengubahan tipe data dalam *dataframe* 43
Gambar 5.16 *Method* untuk memetakan *dataframe output snort* dengan *dataframe labeled flow dataset* 45
Gambar 5.17 Penggabungan *dataset* yang telah dipetakan 46
Gambar 5.18 *Method* untuk mengekspor *dataframe* ke berkas *csv* 47
Gambar 5.19 Proses *input dataset* 47
Gambar 5.20 Tampilan isi *dataframe merged* 47
Gambar 5.21 Jumlah data pada setiap kelas prioritas 48
Gambar 5.22 *One-hot-encoding* dan pemisahan *dataset* 48
Gambar 5.23 Pemuatan pustaka untuk proses *undersampling* 49
Gambar 5.24 Proses *undersampling* 49
Gambar 5.25 Hasil *undersampling* 49
Gambar 5.26 Pemisahan *training set* dan *testing set* 50
Gambar 5.27 Proses penetapan *dataset* skenario 2 50

Gambar 5.28 Pustaka untuk implementasi m*achine learning* 51
Gambar 5.29 Penetapan variabel clfs 51
Gambar 5.30 Pencarian parameter terbaik dengan *GridSearchCV* 52
Gambar 5.31 Parameter dengan skor akurasi terbaik skenario 1 52
Gambar 5.32 Parameter dengan skor akurasi terbaik skenario 2 53
Gambar 5.33 Proses *training classifier* 53
Gambar 5.34 Proses prediksi *data training dan testing* 53
Gambar 5.35 Pustaka untuk menghitung dan menampilkan skor evaluasi 54
Gambar 5.36 Proses menampikan grafik perbandingan skor *GridSearchCV* 55
Gambar 5.37 Proses menampilkan grafik perbandingan skor prediksi data *testing set* dan *training set* 57
Gambar 5.38 Proses menampilkan grafik *confusion matrix* 58
Gambar 5.39 Proses menampilkan grafik perbandingan skor akurasi, *average precision,* dan *average recall* 59
Gambar 5.40 Proses menampilkan grafik perbandingan FPR dan FNR 61
Gambar 5.41 Proses menampilkan grafik perbandingan skor recall alarm *false positive* 62
Gambar 6.1 Grafik komparasi skor akurasi *cross validation* skenario 1 63
Gambar 6.2 Grafik komparasi skor akurasi *cross validation* skenario 2 64
Gambar 6.3 Perbandingan skor evaluasi klasifikasi data *training* dan *testing* 1 65
Gambar 6.4 Perbandingan skor evaluasi klasifikasi data *training* dan *testing* 2 66
Gambar 6.5 *Confusion matrix* skenario 1 67
Gambar 6.6 *Confusion matrix* skenario 2 68
Gambar 6.7 Perbandingan akurasi, *average precision,* dan *average recall* skenario 1 70
Gambar 6.8 Perbandingan FPR dan FNR skenario 1 70
Gambar 6.9 Perbandingan akurasi, *average precision,* dan *average recall* skenario 2 71
Gambar 6.10 Perbandingan FPR dan FNR skenario 2 71
Gambar 6.11 Grafik perbandingan skor recall alarm *false positive* 72

DAFTAR TABEL

Tabel 2.1 Perbandingan Referensi Penelitian 9
Tabel 3.1 Klasifikasi Default *Snort* 13
Tabel 3.2 Statistik *Dataset* ISCX2012 17
Tabel 5.1 Tipe Kelas Serangan Pada *Registered Rules Snort* 36