BAB V
PENUTUP

Kesimpulan serta saran diuraikan oleh penulis dalam bab ini. Kesimpulan berisi rangkuman dari hasil penelitian yang telah dilakukan oleh penulis, sedangkan saran berisi berbagai masukkan penulis untuk penelitian-penelitian berikutnya.

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan oleh penulis, maka dapat ditarik kesimpulan sebagai berikut.

1. Berdasarkan penerapan kombinasi metode *Rangking Importance* dan algoritma *Decision Tree* menghasilkan sembilan fitur penting yang berpengaruh dalam mendeteksi serangan. Sembilan fitur tersebut, antara lain *source ip*, *source port*, *signature id*, *rev*, *signature*, *severity*, *source city name*, *destination regional name*, dan *destination city name*.
2. Akurasi yang diperoleh dengan fitur-fitur penting sebesar 99.97% dengan waktu pelatihan selama 0.021208 s dan waktu pengujian selama 0.001554 s.

5.2 Saran

Beberapa saran yang diberikan oleh penulis untuk penelitian berikutnya yang akan membahas topik yang sama sehingga dapat menghasilkan hasil yang lebih baik adalah sebagai berikut.

1. Menggunakan data *log* lain, seperti data *log* IDS dengan jenis HIDS (Host Based IDS) dan data *log* IPS (*Intrusion Prevention System*). Selain itu, juga dapa menggunakan data mentah yang berasal dari PCAP agar dapat memperoleh *rule* baru berdasarkan algoritma atau metode yang telah diterapkan.
2. Melakukan perbandingan dengan algoritma atau metode yang berbeda sehingga dapat menghasilkan hasil prediksi dan fitur-fitur yang lebih optimal.
3. Membuat sistem yang dapat mendeteksi anomali serangan.