BAB IV
PENUTUP

4.2 Kesimpulan

1. Implementasi Suricata mampu mendeteksi berbagai jenis ancaman seperti DoS, DDoS, dan malware secara dini, membantu meminimalisir dampak serangan terhadap jaringan Dinkominfo sehingga dengan adanya sistem peringatan real-time, Suricata memfasilitasi respons yang cepat terhadap ancaman yang terdeteksi, sehingga mengurangi risiko kerusakan yang lebih besar pada infrastruktur jaringan.
2. Konfigurasi aturan deteksi (*rules*) pada Suricata sangat mempengaruhi hasil deteksi serangan, sehingga dapat menentukan dan menyesuaikan tipe serangan yang ingin di monitor dan dapat membatu para pengembang keamanan server.
3. Dokumentasi yang komprehensif dan pelatihan yang telah diberikan kepada para staf, Dinkominfo kini memiliki kesiapan yang lebih kuat dalam menghadapi ancaman siber, serta kemampuan yang mumpuni untuk mengelola dan merawat sistem IDS secara efisien dalam jangka waktu panjang.

4.2 Saran

1. Agar lebih optimal IDS perlu di install kedalam OPNsense agar bisa mendapatkan hasil yang lebih baik dan fitur yang lebih lengkap.
2. Menambahkan beberapa aturan baru yang dibutuhkan untuk menyesuaikan dengan perkembangan teknologi agar system keamanan tetap berjalan dengan baik.
3. Menambahkan fitur IP filter agar bisa melakukan blokir kepada IP yang tidak sesuai dengan aturan yang sudah di dtetapkan pada suricata.