BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan dari analisa hasil pengujian pada bab IV, sistem integrasi yang dirancang menggunakan komponen wazuh, suricata, serta API Telegram efektif memberikan peringatan dini secara *real-time* terhadap beberapa jenis serangan yang diujikan. Sistem aktif mendeteksi serangan berdasarkan perannya masing-masing seperti analisis dari log host oleh wazuh atau analisis lalu lintas jaringan oleh suricata. Komponen wazuh dan suricata dapat mendeteksi serangan jaringan dengan pola yang berbeda dan saling melengkapi.

Penggunaan notifikasi telegram memberikan keuntungan dalam melakukan pemantauan secara *real-time*, yang membuat administrator dapat menyadari dan segera merespon serangan yang terjadi meskipun terdapat jeda rata-rata sekitar 1 detik antara deteksi Suricata hingga log muncul di dashboard Wazuh..

Upaya tuning rules yang dilakukan pada evaluasi juga membantu mengurangi jumlah alert yang tidak relevan meskipun masih menyisakan beberapa keterbatasan seperti potensi *false positive*. Secara keseluruhan, penelitian ini menunjukkan bahwa integrasi Wazuh, Suricata, dan Telegram dapat menjadi solusi monitoring keamanan jaringan yang efektif, terutama dalam mendeteteksi serangan dan manajemen *event*.

5.2 Saran

Dalam penelitian ini, identifikasi atau analisis serangan oleh sistem hanya sebatas pada 4 jenis serangan, sehingga saran penelitian selanjutnya adalah untuk dapat melakukan pengembangan sistem agar dapat mendeteksi malware atau script judi online dan membuat sistem melakukan *active response* terhadap anomali atau mitigasi secara otomatis.