BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil implementasi, dan pengujian sistem monitoring keamanan server menggunakan Wazuh, Elastic Stack, dan notifikasi Telegram, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Sistem monitoring berhasil diintegrasikan dengan menggabungkan Wazuh dengan Elastic Stack serta bot Telegram sebagai sarana pengiriman notifikasi.
2. Hasil pengujian menunjukkan bahwa Wazuh mampu mendeteksi seluruh serangan pada IP lokal. Namun untuk pengujian Wazuh pada IP publik hanya dapat mendeteksi 4 jenis serangan yaitu SQL *Injection*, XSS *attack*, Malware dan *File Integrity Tampering*. Kemudian notifikasi melalui bot Telegram berhasil melaporkan hasil serangan.

5.2 Saran

Pada Subbab ini menjelaskan beberapa saran untuk perkembangan penelitian selanjutnya sebagai berikut.

1. Pengembangan rule tambahan untuk meningkatkan cakupan deteksi serangan, direkomendasikan untuk menambahkan rule tambahan pada konfigurasi Wazuh dan melakukan Tindakan blokir IP secara otomatis.
2. Penerapan pada lingkungan produksi karena sistem ini sangat potensial untuk diterapkan pada lingkungan produksi dengan adaptasi konfigurasi yang disesuaikan. Dapat ditambahkan mengintegrasikan dengan sistem lain seperti email, SIEM Tingkat lanjut, atau platform manajemen keamanan lainnya untuk cakupan yang lebih luas.