BAB V
SIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, dapat disimpulkan bahwa pengembangan sistem *active response* berbasis Wazuh telah berhasil diimplementasikan sebagai sebuah solusi keamanan siber yang efektif. Sistem ini sukses menciptakan mekanisme otomatis untuk mendeteksi dan merespon ancaman *malware*, dengan memanfaatkan integrasi layanan VirusTotal API untuk meningkatkan akurasi deteksi serta Telegram Bot untuk notifikasi secara *real-time.* Dari segi performa, sistem menunjukkan kinerja yang sangat baik dengan kemampuan mencapai tingkat akurasi deteksi 100% terhadap *file* uji *malware* (EICAR) di semua *platform* yang diuji, yaitu Ubuntu, Windows, dan CentOS.

Sistem *active response* terbukti sangat cepat, meskipun terdapat perbedaan karakteristik antar sistem operasi. *Agent* III (CentOS) menjadi yang paling cepat dengan waktu rata-rata 2,010 detik, karena performa pada saat mendeteksi dan melakukan mitigasi secara lokal sangat konsisten dan stabil, diikuti oleh *agent* I (Ubuntu) dengan 2,118 detik, dengan selisih 0,108 detik dari CentOS dan *agent* II (Windows) sebagai yang paling lambat dengan 2,895 detik, yang utamanya disebabkan oleh, *overhead* sistem operasi Windows saat eksekusi skrip *malware* secara lokal. Selain itu, integrasi notifikasi *real-time* melalui Telegram juga berjalan dengan sangat andal. Sistem mampu mengirimkan laporan peringatan ke Telegram dalam rentang waktu 1–2 detik setelah proses mitigasi ancaman selesai. Notifikasi tersebut menyajikan informasi yang detail dan akurat mencakup tingkat keparahan ancaman, *Rule* ID, nama *agent*, *path file,* dan *timestamp* yang membuktikan kemampuan pelaporan sistem yang cepat dan relevan untuk mendukung pengambilan keputusan tim keamanan secara segera

5.2 Saran

Berdasarkan hasil penelitian dan analisis yang diperoleh, beberapa saran yang dapat diajukan untuk penelitian selanjutnya adalah Untuk pengembangan di masa depan, penelitian ini sebaiknya diposisikan sebagai landasan fundamental untuk membangun solusi keamanan siber yang lebih komprehensif. Disarankan agar sistem deteksi intrusi berbasis HIDS ini dilanjutkan dengan memperkuat integrasi pada layanan eksternal seperti Wazuh dan VirusTotal API, guna menciptakan mekanisme deteksi dan respons ancaman yang sepenuhnya otomatis. Namun, setelah matang, pengembangan teknis ini wajib divalidasi secara ketat dengan mengujinya dalam lingkungan produksi yang kompleks. Uji coba tersebut harus mencakup skenario krusial seperti integrasi penuh dengan sistem SIEM korporat untuk visibilitas terpusat, serta pengujian ketahanan terhadap varian *malware* baru dan canggih untuk membuktikan keandalannya.

Setelah terbukti andal, langkah selanjutnya adalah memastikan sistem ini diadopsi sepenuhnya ke dalam alur kerja operasional harian. Kapabilitas notifikasinya perlu diperluas agar terhubung dengan ekosistem keamanan yang lebih luas, seperti *platform ticketing* (misalnya Jira atau ServiceNow) untuk memastikan setiap insiden terdokumentasi dan ditangani secara terstruktur. Selain itu, penyaluran informasi ke *dashboard* keamanan terpusat akan memberikan visibilitas penuh bagi tim dan manajemen. Dengan demikian, sistem ini bertransformasi dari sekadar alat deteksi menjadi komponen integral yang mendukung keseluruhan siklus hidup manajemen insiden keamanan di sebuah organisasi.