BAB V
PENUTUP

5.1 Simpulan

Berdasarkan hasil uji coba, integrasi Wazuh dengan *Malware Bazaar* berhasil mendeteksi 4 dari 5 sampel malware yang diuji, dengan akurasi deteksi sebesar 80%. Pengujian dilakukan dengan menambahkan file sample malware ke dalam folder yang dimonitor oleh File Integrity Monitoring (FIM), di mana *Malware Bazaa*r digunakan sebagai referensi untuk mendeteksi keberadaan malware berdasarkan hash yang telah terdaftar dalam database-nya.

Perbandingan dengan VirusTotal menunjukkan bahwa semua sampel malware yang diuji berhasil terdeteksi, berbeda dengan hasil deteksi *Malware Bazaar* yang masih memiliki keterbatasan. Hal ini mengindikasikan bahwa cakupan deteksi *Malware Bazaar* lebih terbatas dibandingkan VirusTotal, yang memiliki lebih banyak sumber data dari berbagai mesin antivirus serta menggunakan metode analisis yang lebih canggih. Salah satu faktor utama yang menyebabkan perbedaan ini adalah ketergantungan *Malware Bazaar* pada hash file sebagai metode identifikasi malware, yang membuatnya sulit mendeteksi malware yang telah mengalami modifikasi atau menggunakan teknik Defense Evasion.

5.2 Saran

Untuk meningkatkan efektivitas deteksi malware dalam sistem yang menggunakan Wazuh, beberapa langkah perbaikan dapat dilakukan, antara lain:

1. Integrasi dengan sumber threat intelligence tambahan

   Selain *Malware Bazaar,* disarankan untuk mengintegrasikan Wazuh dengan sumber lain seperti VirusTotal, MISP *(Malware Information Sharing Platform)*, atau *YARA rules* agar cakupan deteksi menjadi lebih luas dan tidak hanya bergantung pada database hash.

2. Implementasi teknik deteksi tambahan

   Menggunakan metode analisis lain seperti heuristics, signature-based detection, atau sandboxing dapat membantu dalam mengidentifikasi malware yang tidak terdeteksi melalui hash matching saja.

3. Pengujian dengan beragam sampel malware

   Melakukan pengujian dengan sampel malware yang lebih banyak dan beragam, termasuk malware dengan teknik penghindaran deteksi, dapat membantu dalam mengevaluasi keandalan sistem deteksi yang diterapkan.

Dengan penerapan rekomendasi di atas, efektivitas sistem deteksi berbasis Wazuh dapat ditingkatkan, sehingga lebih mampu dalam mengidentifikasi ancaman malware yang semakin kompleks dan berkembang.