BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah dilakukan analisis terhadap *Security Information and Event Management* (SIEM) Wazuh dengan konfigurasi VirusTotal terhadap serangan *malware*, dapat disimpulkan bahwa:

1. Cara mendeteksi serangan *malware* pada sistem adalah dengan melakukan pemantauan atau *monitoring* sistem itu sendiri dengan memanfaatkan SIEM (*Security Information and Event Management).*
2. Solusi yang tepat bagi penulis untuk mengatasi serangan *malware* adalah dengan melakukan pencegahan masuknya *malware* itu sendiri ke dalam perangkat. Dalam penelitian ini ada sebuah konfigurasi dari Wazuh yang dapat me-*remove* langsung *file malicious* yang baru saja diunduh. Selain itu, detail atau karakteristik dari *malicious file* itu sendiri dapat dilihat berkat konfigurasi antara Wazuh dengan VirusTotal. Pencegahan menggunakan Wazuh sebagai implementasi SIEM ini dapat diberlakukan di perangkat – perangkat individu maupun organisasi agar dapat terbebas dari serangan *malware*.
3. Peran SIEM sebagai *monitoring* terhadap serangan malware menurut penulis cukup baik. Hal ini dapat dibuktikan dari total 50 *malicious file* yang sudah diunduh semuanya dapat terdeteksi dan berhasil di-*remove*, kecuali 5 di antaranya tidak dapat terditeksi oleh Wazuh. Selain itu baiknya peran SIEM dalam *monitoring* terhadap serangan *malware* ini dapat dilihat dari faktor *Security* atau keamanan dengan adanya automasi *remove file*, *Information* atau informasi dengan adanya informasi detail virus berkat konfigurasi VirusTotal, *Event* yaitu adanya *Integrity Monitoring* yang menunjukkan kejadian yang terjadi secara langsung (*real time*) dan

Management yaitu memusatkan suatu direktori untuk proses *monitoring*. Selain itu, Wazuh sebagai implementasi SIEM di sini terbukti dapat menjadi pengganti dari *Anti-Malware* berbayar yang ada di luar sana. Hal ini dibuktikan dari persentase dari hasil konfigurasi antara Wazuh dengan VirusTotal mencapai 90%.

5.2 Saran

Saran penulis untuk penelitian selanjutnya adalah menambah lagi jumlah *malware* dalam pengujian agar terbukti lebih baik lagi bahwa wazuh sebagai implementasi SIEM menjadi pilihan tepat untuk mencegah terjadinya serangan *malware* pada perangkat.