BAB V
PENUTUP

5.1 KESIMPULAN

Setelah dilakukan penelitian mengenai pendeteksian serangan *Distributed Denial of Service* menggunakan *Security Information and Event Management* (SIEM) dengan menggunakan log sistem pada dua buah sistem operasi, dapat disimpulkan bahwa.

1. Untuk mendeteksi apakah sistem mengalami serangan *Distributed Denial of Service*, langkah yang dapat diambil adalah secara rutin memantau sistem dan mengamati tanda-tanda yang menunjukkan terjadinya serangan tersebut.
2. Melalui penelitian ini, hanya ciri-ciri serangan *Distributed Denial of Service* yang dapat dideteksi oleh SIEM. Ciri-ciri tersebut mencakup lonjakan tajam dalam penggunaan sumber daya, peningkatan yang signifikan dalam jumlah paket yang diterima oleh perangkat Host, dan interval waktu yang sangat singkat antara penerimaan satu paket dengan paket lainnya. Hasil penelitian menunjukkan bahwa percobaan yang dilakukan berhasil dikategorikan sebagai serangan *Distributed Denial of Service*. Penulis melakukan analisis karena SIEM hanya dapat menangkap ciri-ciri dari serangan *Distributed Denial of Service*.
3. SIEM dapat membantu berbagai organisasi, termasuk Organisasi Kecil, dalam mengatasi kejahatan siber melalui pemantauan berkala pada SIEM yang sebelumnya telah dikonfigurasi agar sesuai dengan kebutuhan organisasi. Selain itu, penelitian ini fokus pada pemahaman tentang serangan *Distributed Denial of Service*. Dalam penelitian ini, penulis menggunakan SIEM open-source yang tetap memiliki kemampuan pemantauan, cocok untuk organisasi dengan investasi infrastruktur jaringan yang terbatas. Dibandingkan dengan SIEM lain, Wazuh memiliki kemampuan yang lebih luas untuk melakukan

pemantauan, termasuk deteksi serangan *Distributed Denial of Service* dan anomaly-anomali lainnya yang mengindikasikan kejahatan siber.

5.2 SARAN

Menurut penelitian ini, untuk mengatasi *Distributed Denial of Service*, diperlukan langkah-langkah sebagai berikut: melakukan pemantauan rutin pada sistem, mengenali ciri-ciri dari serangan *Distributed Denial of Service* melalui proses monitoring, mengkonfigurasi SIEM sesuai dengan studi kasus *Distributed Denial of Service*, dan meningkatkan pemahaman mengenai *Distributed Denial of Service*.

Untuk penelitian selanjutnya, penulis menyarankan agar penggunaan *tools* SIEM yang digunakan dapat dimaksimalkan. Selain itu, disarankan untuk memberikan konfigurasi tambahan guna menghindari terjadinya *false* positif, sehingga proses pemantauan dapat mencapai tingkat efektivitas yang maksimal.