BAB 5
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Setelah melakukan analisis pada log Mikrotik dan melakukan penelitian seperti yang telah diuraikan diatas, maka dapat disimpulkan bahwa penelitian ini berfokus pada kapabilitas dan kapasitas MikroTik sebagai node yang mengirimkan data log ke pihak ketiga yaitu Splunk dalam upaya mendeteksi dan mengelola serangan pola trafik yang mencurigakan. Dengan menggunakan perangkat MikroTik Router dan alat analisis log seperti Splunk, penelitian ini berhasil mengidentifikasi berbagai serangan, termasuk DNS *Flood*, SMB *Flood*, Telnet F*lood*, SSH *Flood*, dan serangan Metasploit. Penerapan aturan firewall di MikroTik terbukti efektif dalam menangkap dan mencatat aktivitas mencurigakan. Hasil analisis log menunjukkan pola serangan yang konsisten pada waktu tertentu, dengan puncak aktivitas pada menit ke-40 dalam setiap jam.

Jadi dari hasil deteksi anomali yang sudah menunjukan bahwa pada menit ke-40 memiliki 538 *event* (97.996%), sementara menit lainnya memiliki jauh lebih sedikit event, ini terjadi karena adanya aktivitas yang tidak biasa atau serangan yang terfokus pada menit tersebut.

5.2 SARAN

Berdasarkan penelitian seperti yang telah diuraikan ditas, ada beberapa saran untuk meningkatkan analisis dan mitigasi serangan terhadap jaringan. Di antaranya yaitu:

1. Penelitian selanjutnya dapat mempertimbangkan untuk menggunakan sumber data log yang lebih beragam seperti log dari perangkat jaringan lainnya, server, dan aplikasi untuk mendapatkan gambaran tentang pola serangan.
2. Melakukan studi kasus pada berbagai jenis lingkungan, untuk melihat bagaimana pendekatan yang digunakan dalam penelitian ini dapat diterapkan atau disesuaikan.