BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian Implementasi Sistem Keamanan Jaringan Dengan Deteksi Serangan *Denial of Service* dan *Brute-Force* Pada Router MikroTik Dengan Notifikasi Melalui Whatsapp yang telah dilakukan maka didapatkan beberapa kesimpulan sebagai berikut:

a. Metode IDS (*Intrusion Detection System*) yang diimplementasikan pada router MikroTik dengan menggunakan *firewall RAW* terbukti efektif untuk menghentikan serangan *Brute-Force*. Hal ini dibuktikan dengan pesan kesalahan yang menunjukkan ketidakmampuan untuk terhubung ke server yang diserang.
b. Meskipun metode IDS (*Intrusion Detection System*) yang diimplementasikan pada router MikroTik dengan menggunakan *firewall RAW* berhasil mengurangi penggunaan CPU secara signifikan dari serangan *Ping Flood* dan *SYN Flood* namun belum mampu untuk memblokir serangan tersebut.
c. Notifikasi serangan *Brute-Force* memerlukan waktu yang relatif cepat sekitar 2-3 detik.
d. Notifikasi serangan *Ping Flood* dan *SYN Flood* membutuhkan waktu pengiriman yang lebih bervariasi dengan rentang waktu antara 1-4 detik untuk serangan *Ping Flood* dan 2-6 detik untuk serangan *SYN Flood*.

5.2 Saran

Berikut merupakan beberapa masukan dari penulis yang dapat digunakan sebagai tinjauan dimasa depan:

a. Evaluasi ulang terhadap konfigurasi *firewall RAW* untuk meningkatkan kemampuan *firewall* dalam menghadapi serangan *Ping Flood* dan *SYN Flood*.
b. Melakukan peninjauan mendalam terhadap sistem notifikasi dan mengidentifikasi sumber masalah, kemudian menerapkan solusi yang tepat agar notifikasi hanya dikirimkan sekali saat terjadi kejadian yang memicu notifikasi.
c. Melakukan pemantauan secara terus-menerus terhadap kinerja *firewall* dan sistem keamanan secara keseluruhan serta perbaruan rutin perangkat lunak dan konfigurasi *firewall* untuk menghadapi ancaman keamanan yang terus berkembang.