

BAB 5

PENUTUP

5.1 KESIMPULAN

Berdasarkan pada hasil penelitian dan perhitungan yang dilakukan pada penelitian ini, maka dapat diambil kesimpulan seperti berikut.

- a. Serangan DDOS dari aplikasi LOIC menyerang kondisi *traffic* akses *web server* yang membuat nilai *delay* yang terjadi sebesar 2,86 detik (tidak menjamin semua akses berhasil), *packet loss* mencapai 99,79% (dari total paket yang dilewatkan pada layanan *web server*) dan *throughput* hanya mencapai 337 bps (akibat *traffic* dipadati serangan DDOS).
- b. Sistem keamanan memblokir semua pengiriman paket SYN dan semua paket di protokol ICMP yang dikirim dari alamat penyerang serta menonaktifkan *port* aktif yang tidak terpakai tanpa ikut memblokir akses layanan *web server*.

5.2 SARAN

Penelitian ini memiliki beberapa saran untuk perkembangan pada implementasi ataupun pembahasan secara langsung bagi penelitian selanjutnya seperti berikut.

- a. Rancangan sistem keamanan dengan *proxy server squid* dan *firewall iptables* ini diimplementasikan pada jenis serangan DDOS lainnya (selain *syn-flooding*).
- b. Penerapan eksekusi serangan DDOS dengan jenis *syn-flooding* ini diimplementasikan pada layanan lain (selain *web server*) yang menyangkut segi *availability* dari keamanan jaringan.
- c. Rancangan pengamanan *web server* ini diimplementasikan dengan jenis serangan selain DDOS untuk melihat penanganan serangan dengan keamanan jaringan dari segi *confidentiality* ataupun *integrity*.
- d. Perlu penggunaan dan implementasi langsung dengan perangkat asli dalam penerapan sistem keamanan ini sehingga kestabilan sistem dan keakuratan data dapat terjamin.