

BAB V PENUTUP

5.1 Kesimpulan

Dari hasil penelitian yang dilakukan oleh peneliti dengan judul analisis dan implementasi keamanan jaringan *file transfer protocol* (FTP) menggunakan *intrusion prevention system* (IPS) pada MikroTik. Sistem yang dibangun dapat berjalan dengan lancar dan berjalan dengan baik sesuai dengan tujuan dari penelitian ini. Adapun kesimpulan yang didapatkan yaitu sebagai berikut :

1. Dari pengujian yang dilakukan menggunakan 3 serangan yaitu : *Brute force* FTP, *DDoS ICMP flood*, dan *Port scanning*. Mendapatkan hasil sebagai berikut : Pertama serangan *brute force* FTP menggunakan tools ncrack dan xHydra dengan pengujian sebanyak 30 kali, lalu durasi waktu serangan rata-rata yang diperlukan yaitu 50,41 detik dan 100,6 detik. Hasil yang didapatkan setelah menerapkan rules IPS pada *firewall* yaitu serangan *brute force* FTP tidak mampu mendapatkan akses username dan password FTP atau tingkat keberhasilannya adalah 0. Kedua pada serangan *port scanning* menggunakan aplikasi znmip dengan pengujian sebanyak 30 kali, lalu rata-rata waktu yang diperlukan scanning yaitu 103.3 detik. Didapatkan hasil dari 30 kali pengujian 7 kali status pada port 21 terbuka, walaupun status port 21 terbuka rules IPS pada *firewall* masih tetap berjalan dan melakukan prevention dengan memblacklist dan mendrop IP penyerang maka serangan yang dilakukan tetap gagal. Ketiga pada serangan *DDoS ICMP flood* menggunakan tools Hping3 dengan pengujian 15 kali sebelum dan sesudah menerapkan IPS, hasil yang didapat yaitu sebelum menerapkan rules IPS CPU load saat terjadi serangan naik dari 63% - 100% yang membuat server menjadi lambat saat menerima request client dan server down. Hasil setelah menerapkan rules IPS pada *firewall* CPU load hanya naik 13% - 36% saat terjadi serangan yang membuat server tetap stabil walaupun terjadi serangan dan membuat request client ke server tetap berjalan lancar.
2. Respon time yang dibutuhkan untuk melakukan prevention dan mengirim pesan alert peringatan ke gmail untuk administrator menggunakan percobaan pengujian 3 serangan dengan menerapkan sistem IPS pada *firewall* MikroTik

didapatkan hasil respon time yaitu 2 Detik – 5 Detik, hasil respon time tersebut bisa digolongkan sebagai *real-time*.

5.2 Saran

1. Untuk penelitian kedepanya bisa menambahkan metode seperti *port knocking* atau sistem *certificate* TLS untuk menambah kemanan pada service FTP server di router MikroTik menjadi lebih *secure*.
2. Untuk penelitian selanjutnya bisa ditambahkan serangan yang berbeda seperti *sniffing* atau DDoS tipe lain.
3. Untuk penelitian kedepanya bisa menambahkan mode sampel/sampling pengujian untuk mendapat hasil yang lebih akurat dan untuk serangan DDoS tambahkan dasar teori mengenai penggunaan cpu load agar lebih detail.

