BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan dengan analisa dan pengujian yang telah dilakukan, dengan adanya laporan skripsi yang berjudul "*Auto Capture* File Log Pada *Intrusion Prevention System* (IPS) Saat Terjadi Serangan Pada Jaringan Komputer" dapat diambil kesimpulan :

1. Serangan dapat terdeteksi dan dicegah tergantung pola serangan tersebut ada di dalam *rule Intrusion Prevention System* atau tidak. Pengelola *Intrusion Prevention System* harus mengupdate rule terbaru di snort.conf untuk menahan serangan.
2. Jenis serangan seperti *Ping of Death* pada rancangan yang dibuat dapat dicegah dengan menggabungkan tool Snort dan Iptables.
3. Snort dan Iptables yang dirancang belum bisa mencegah serangan *Ping of Death* dari banyak *IP Address* dikarenakan pengimputan *IP Address attacker* ke dalam rule Snort masih manual.
4. Informasi yang didapat dari hasil serangan dapat langsung dicetak sebagai bukti dokumentasi bahwa telah terjadi serangan untuk penindakan lebih lanjut oleh *administrator.*

5.2 Saran

Pada penulisan skripsi ini tentu masih terdapat banyak kekurangan, yang mungkin dapat disempurnakan lagi pada pengembangan selanjutnya, terdapat saran yang dapat dipergunakan kedepannya, antara lain :

1. Snort sebagai salah satu tool sistem keamanan jaringan untuk mencegah serangan seperti *Ping of Death* hendaknya dapat dikembangkan tidak hanya memblock *traffic data* dari 1 *IP Address* saja, tetapi bisa lebih banyak lagi, seperti block DDoS *(Distribute Denial of Service)*.
2. *Intrusion Prevention System* hendaknya dapat dikembangkan untuk mencegah serangan-serangan yang dapat membahayakan server lain, seperti *Port Scanners, Password Guessing, Backdoor,* dan lain sebagainya.
3. Penambahan modul-modul lain yang mendukung kinerja *Intrusion Prevention System* akan membantu efisiensi kerja sistem, seperti update otomatis rule-rule snort dari sumbernya dan juga penambahan *front-end*.