

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan analisa dan pengujian sistem yang telah dilakukan dengan judul penelitian “Analisis Dan Perancangan Sistem Keamanan Jaringan Menggunakan NIPS (*Network-based Intrusion Prevention System*) Dengan Metode *Signature Based System*” dapat di ambil beberapa kesimpulan sebagai berikut :

1. Bahwa Network Intrusion Prevention Sistem (IPS) dapat digunakan sebagai salah satu cara untuk mengamankan server dengan cara monitoring lalu lintas jaringan dan menghentikan paket data yang berbahaya berdasarkan pada aturan atau signature base yang telah diterapkan.
2. Rancangan IPS Server berhasil melakukan pencegahan terhadap serangan yang telah ditentukan dalam skenario pengujian. Pengujian meliputi Port scanning, DoS, dan ssh bruteforce.
3. Hasil intrusi yang telah sistem Snort deteksi dapat dilihat melalui GUI berbasis web Snorby.

5.2 Saran

Penulis menyadari bahwa masih banyak kekurangan dalam penelitian ini, yang mungkin dapat dijadikan referensi dan disempurnakan lagi untuk pengembangan penelitian selanjutnya. Untuk itu ada beberapa saran yang dapat membantu rencana pengembangan selanjutnya agar mendapatkan hasil yang lebih

baik yaitu sebagai berikut :

1. Penambahan aturan atau rule base untuk berbagai macam serangan perlu dilakukan agar kelemahan sistem tidak dapat terdeteksi.
2. Lebih memahami dan mendalami serta mengembangkan logika pembuatan rules snort agar mampu memperoleh rules yang efisien dan akurat dalam mendeteksi setiap jenis serangan.
3. Dilakukan pengujian dengan jenis serangan lainnya seperti SQL injection, XSS, virus, penanaman hingga akses backdoor atau menggunakan teknik yang lebih mendalam seperti contohnya ketika menggunakan nmap perlu dilakukan ujicoba dengan stealth scanning, intense scanning, decoy scanning agar bisa menentukan rules yang lebih tepat dan akurat.

