DAFTAR ISI

BAB I PENDAHULUAN 1

1.1 Latar Belakang Penelitian 1

1.2 Identifikasi Masalah 4

1.2.1 Rumusan Masalah 4

1.2.2 Batasan Masalah 4

1.3 Tujuan dan Manfaat Penelitian 4

1.3.1 Tujuan Penelitian 4

1.3.2 Manfaat Penelitian 5

1.4 Sistematika Penulisan 5

BAB II TINJAUAN PUSTAKA 7

2.1 Jaringan Komputer 7

2.1.1 Jenis Jaringan Komputer 8

2.1.2 Protokol Jaringan Komputer 8

2.1.3 Model OSI 10

2.2 Keamanan Jaringan Komputer 13

2.3 Tipe Serangan Keamanan Komputer 14

2.4 Risiko Jaringan Komputer 15

2.5 Jenis – Jenis Serangan Jaringan Komputer 16

2.5.1 Denial of Service (DoS) 16
2.5.2 Port Scanning 17
2.5.3 IP Spoofing 18
2.5.4 Malware (Virus) 18
2.6 Intrusion Detection System 18
2.6.1 Jenis – Jenis IDS 18
2.6.2 Fungsi IDS 19
2.6.3 Metode IDS 21
2.7 Snort 24
2.8 Penelitian Sebelumnya 24
BAB III METODE PENELITIAN 27
3.1 Tahapan Penelitian 27
3.2 Analisis Kebutuhan Sistem 29
3.2.1 Analisis Kebutuhan Perangkat Keras 29
3.2.2 Analisis Kebutuhan Perangkat Lunak 30
3.3 Rancangan Sistem 30
3.4 Signature Anomali Based (SAB) 32
3.4.1 Penentuan Baseline Jaringan Normal 35
3.4.2 Penggunaan Rule Database Signature Serangan 36
3.5 Skenario Pengujian 36

3.6 Pengukuran Kinerja IDS 38
3.6.1 Parameter Gangguan 38
3.6.2 Parameter Responsi IDS 38
3.6.3 Parameter Komputasi 39
3.6.4 Pengujian Serangan Dengan Digital Blaster 39
3.6.5 Pengujian Metode Signature Based 40
3.6.6 Pengujian Metode Anomali Based 41
3.6.7 Pengujian Metode Signature Anomali Based (SAB) IDS 42
3.7 Teknik Analisis Data 43
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 44
4.1 Hasil Pengukuran Aktifitas Serangan 44
4.1.1 Hasil Pengujian Serangan Dengan Anomali Based 44
4.1.2 Hasil Pengujian Serangan Dengan Signature Based 45
4.1.3 Hasil Pengujian Serangan Dengan SAB IDS 46
4.1.4 Hasil Pengukuran Jumlah Serangan Dengan Anomali Based 47
4.1.5 Hasil Pengukuran Jumlah Serangan Dengan Signature Based 48
4.1.6 Hasil Pengukuran Jumlah Serangan Dengan SAB IDS 50
4.2 Hasil Pengukuran Uji Responsi 51
4.3 Hasil Pengukuran Komputasi Sumber Daya 52
4.3.1 Hasil Pengukuran Komputasi Anomali Based 52

4.3.2 Hasil Pengujian Komputasi Signature Based 53
4.3.3 Hasil Pengujian Komputasi Signature Anomali Based (SAB) 54
4.4 Analisis Data 55
4.4.1 Aktifitas Serangan 55
4.4.2 Penggunaan Memori 60
4.4.3 Penggunaan Processor (CPU) 61
4.4.4 Analisa Tingkat Error 63
BAB V KESIMPULAN DAN SARAN 67
5.1 Kesimpulan 67
5.2 Saran 68