DAFTAR ISI

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI v
DAFTAR GAMBAR x
DAFTAR TABEL xv
DAFTAR SIMBOL xviii
DAFTAR LAMPIRAN xix
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Perumusan Masalah 2
1.3 Maksud dan Tujuan 3
1.4 Batasan Masalah 4
1.5 Metodologi Penelitian 4
1.6 Sistematika Penulisan 6
BAB 2 TINJAUAN PUSTAKA 9
2.1 Jaringan Komputer 9
2.1.1 Jenis Jaringan Komputer 9
2.1.2 Arsitektur Jaringan Komputer 10
2.2 Protokol Jaringan Komputer 10
2.2.1 Model Referensi OSI 10
2.2.2 Protokol TCP/IP 15
2.2.2.1 Layanan TCP/IP 15
2.2.2.2 Arsitektur TCP/IP 16
2.3 Lapisan Pada Protokol *Network* 20
2.3.1 IP Layer 20
2.3.2 TCP Layer 21
2.3.3 IP (*Internet Protocol*) 21
2.3.3.1 IP Protocol Lapisan Atas 21

2.3.3.1.1 *Transmission Control Protocol* (TCP) 21
2.3.3.1.2 User Datagram Protocol (UDP) 24
2.3.3.1.3 *Internet Control Message Protocol* (ICMP) 25
2.4 Perangkat Jaringan Komputer 26
2.4.1 Kabel *Unshielded Twisted Pair* (UTP) 27
2.4.2 *Switch* 28
2.4.3 *Network Interface Card* (NIC) 29
2.5 Keamanan Jaringan Komputer 30
2.5.1 Tujuan Keamanan Jaringan Komputer 31
2.5.2 Tipe Ancaman Keamanan Sistem Komputer 31
2.5.3 Bentuk Ancaman Jaringan Komputer 32
2.6 Jenis Serangan Jaringan Komputer 33
2.6.1 *Port Scanning* 33
2.6.2 *Teardrop* 33
2.6.3 IP *spoofing* 33
2.6.4 ICMP *flood* 34
2.6.5 UDP *flood* 34
2.6.6 *Packet interception* 34
2.6.7 Smurf *attack* 35
2.6.8 DOS (*Denial Of Service*) 35
2.6.9 SQL *Injection* 37
2.6.10 *Cross Site Scripting* 37
2.7 *Intrusion Detection System* 38
2.7.1 Jenis *Intrusion Detection System* 38
2.7.2 Metode Pada *Intrusion Detection System* 39
2.8 Snort 40
2.8.1 Komponen Snort 40
2.9 Basis Data 42
2.10 PHP 42
2.11 CSS 43
2.12 MySQL 43

BAB 3 ANALISIS DAN PERANCANGAN....45
3.1 Analisis....45
3.1.1 Analisis Masalah....45
3.1.2 Analisis Metode Serangan....47
3.1.2.1 Analisis *Footprinting*....49
3.1.2.2 Analisis Scanning....49
3.1.2.3 Analisis serangan *Distributed Denial Of Service* (DDOS)....53
3.1.2.4 SQL *injection*....59
3.1.2.5 *Cross Site Scripting*....68
3.1.3 Analisis Metode Deteksi Serangan....69
3.1.3.1 Analisis *Intrusion Detection System*....69
3.1.3.1.1 *Anomaly vs. Signature*....71
3.1.3.1.2 *Host vs. Network*....74
3.1.3.1.3 *Centralised vs. Distributed*....77
3.1.3.1.4 *Audit Trail vs. Network Packets*....79
3.1.3.1.5 *Active vs. Passive*....79
3.1.3.1.6 *Real time vs. Interval-based*....80
3.1.3.2 Analisis Pemilihan Intrusion Detection System....80
3.1.3.3 Analisis *Intrusion Detection System* Snort....84
3.1.3.4 Analisis Proses Pada Snort....87
3.1.3.4.1 Analisis Pcap....88
3.1.3.4.2 Analisis *Decoder*....93
3.1.3.4.3 Analisis *Preprocessors*....94
3.1.3.4.4 Analisis *Rules Files*....97
3.1.3.4.5 Analisis *Detection Engine*....100
3.1.3.4.6 Analisis *Logging* and *Alerting System*....107
3.1.4 Analisis Kebutuhan Infrastruktur....109
3.1.4.1 Kebutuhan Perangkat Keras....109
3.1.4.2 Kebutuhan Perangkat Lunak....110
3.2 Perancangan Sistem....111
3.2.1 Perancangan Arsitektur Simulasi....111

3.2.2 Perancangan Arsitektur Pengujian 111
3.2.3 Perancangan *Rules* 112
3.2.3.1 Perancangan Rule SQL *injection* 113
3.2.3.2 Perancangan *Rule Cross Site Scripting* 113
3.2.3.3 Perancangan Rule *Port Scanning* 114
3.2.3.4 Perancangan Rule DDOS 115
3.2.4 Perancangan Proses Pengujian dan *Assesment* 116
3.2.4.1 Perancangan Pengujian dan Penilaian Kecepatan Akses 116
3.2.4.2 Perancangan Pengujian Ketepatan Deteksi Serangan 117
3.2.5 Perancangan Aplikasi Monitoring IDS 118
3.2.5.1 Perancangan Basis Data 118
3.2.5.2 Perancangan Antarmuka Pengguna 121
3.2.5.3 Perancangan Pesan 125
3.2.5.4 Perancangan Jaringan Semantik 127
3.2.5.5 Perancangan Prosedural 127
BAB 4 IMPLEMENTASI DAN PENGUJIAN 131
4.1 Implementasi 131
4.1.1 Implementasi Arsitektur Jaringan Pengujian 131
4.1.1.1 Implementasi Perangkat Keras 132
4.1.1.2 Implementasi Perangkat Lunak 134
4.1.1.3 Implementasi dan Konfigurasi Arsitektur Jaringan 135
4.1.2 Implementasi Aplikasi 139
4.1.2.1 Implementasi Snort 139
4.1.2.2 Implementasi *Rules* Snort 143
4.1.2.3 Implementasi Basis Data Snortbow 145
4.1.2.4 Implementasi Antar Muka Snortbow 148
4.2 Pengujian 151
4.2.1 Pengujian Arsitektur Jaringan 151
4.2.1.1 Pengujian Keterhubungan Antar Perangkat 151
4.2.2 Pengujian dan Penilaian IDS Snort 153
4.2.2.1 Pengujian dan Penilaian Kecepatan Akses 153