DAFTAR ISI

LEMBAR PENGESAHAN ..... **ii**
LEMBAR PERNYATAAN ORISINALITAS ..... **iii**
ABSTRACT ..... **v**
ABSTRAK ..... **vi**
KATA PENGANTAR ..... **vii**
UCAPAN TERIMA KASIH ..... **viii**
DAFTAR ISI ..... **x**
DAFTAR GAMBAR ..... **xiii**
DAFTAR TABEL ..... **xv**
DAFTAR SINGKATAN ..... **xvi**
DAFTAR ISTILAH ..... **xvii**

BAB I PENDAHULUAN
1.1 Latar Belakang **1**
1.2 Rumusan Masalah **2**
1.3 Tujuan Penelitian **2**
1.4 Batasan Masalah **2**
1.5 Metodologi Penelitian **3**
1.6 Sistematika Penulisan **4**

BAB II DASAR TEORI
2.1 *Intrusion Detection System* (*IDS*) **5**
2.1.1 Definisi 5
2.1.2 Jenis-jenis IDS 5
2.1.3 Cara Kerja IDS Mengenali Adanya *Intruder* 7
2.2 *SNORT* **8**
2.2.1 Definisi 8
2.2.2 Komponen IDS *Snort* 9
2.3 *Linux* **13**
2.3.1 Definisi 13
2.4 *Network Security* **13**
2.4.1 Definisi 13

2.5 *MySql* 14
2.5.1 Definisi 14
2.5.2 Jenis-jenis Tipe Data 15

BAB III ANALISIS DAN PERANCANGAN
3.1 Desain Sistem Utama 18
3.1.1 Desain Subproses Sistem Penyaringan Paket Data 19
3.1.2 Desain Subproses Sistem *Alert Administrator* 20
3.2 Alur Perancangan 20
3.3 Spesifikasi Perangkat yang Dibutuhkan 21
3.3.1 Komponen Perangkat Keras Minimum (*Hardware*) 21
3.3.2 Komponen Perangkat Lunak (*Software*) 21
3.4 Instalasi dan Konfigurasi Jaringan 22
3.4.1 Topologi Jaringan 22
3.4.2 Instalasi dan Konfigurasi Linux Debian Lenny 5.0.4 22
3.4.3 Instalasi dan Konfigurasi IDS 23
3.5 Perancangan Web PHP 26
3.5.1 Desain *Input* 26
3.6 Desain Sistem 28
3.6.1 Pembuatan User Interface PHP untuk Email Notification 29
3.7 Arsitektur Monitoring Sistem 30
3.8 Skenario Pengujian 31
3.8.1 Konfigurasi awal sebelum melakukan serangan 31
3.8.2 Proses yang dilakukan penyerang 32
3.8.3 Peringatan *Email* 32

BAB IV IMPLEMENTASI DAN PENGUJIAN
4.1 Pengujian Sistem 34
4.1.1 Serangan 1 *Scanner* 34
4.1.2 Serangan 2 *Ping Attack* 35
4.1.3 TCP and UDP Flood 37
4.1.4 Syn FIN 38
4.1.5 Serangan 3 *Syn Attack* 40
4.1.6 Serangan 6 Virus Eicar 41
4.1.7 Pengujian Performansi Sistem 43
4.2 Kesimpulan Kerja Sistem 43
4.3 Kesimpulan Performansi Sistem 46

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan 48

5.2 Saran 49

DAFTAR PUSTAKA 50

LAMPIRAN A Instalasi dan Konfigurasi Linux Debian Lenny 5.0.4

LAMPIRAN B Instalasi dan Konfigurasi *Snort* 2.9.2

LAMPIRAN C Konfigurasi DNS

LAMPIRAN D Konfigurasi *Mail Client* (*Squirrelmail*)

LAMPIRAN E Data Pengujian

LAMPIRAN F *Rules Snort*