

DAFTAR ISI

ABSTRAK	Error! Bookmark not defined.
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xiv
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Perumusan Masalah	2
1.3 Pembatasan Masalah	2
1.4 Tujuan	3
1.5 Sistematika Penulisan	3
BAB II LANDASAN TEORI	5
2.1 Intrusion Detection System	5
2.1.1 Teknologi IDS	5
2.1.2 Jenis-jenis Pendeteksian	7
2.2 Open System Interconnection Model	8
2.3 TCP/IP	9
2.3.1 Model TCP/IP	10
2.4 Denial Of Service Attack	12
2.5 Logika Fuzzy	13
2.5.1 Himpunan Fuzzy	14
2.5.2 Fungsi Keanggotaan	16

2.5.3 Fungsi Implikasi	19
2.5.4 Fuzzy Inference System.....	20
2.6 Database	21
2.7 MySQL.....	22
2.8 PHP	23
BAB III METODE PENELITIAN.....	25
3.1 Perancangan Sistem dan Blok Diagram Sistem	25
3.2 Rancangan Sistem	26
3.2.1 Perancangan Modul Sniffing Paket.....	27
3.2.2 Sampling Data Serangan	29
3.2.3 Perancangan Fuzzy.....	29
3.3 Desain Sistem.....	36
3.3.1 Desain Input	37
3.3.2 Desain Proses	39
3.3.3 Desain Output	40
3.3.4 Desain Autentifikasi.....	41
3.4 Implementasi Program	42
3.4.1 Pengumpulan Data (<i>Database Log Snort</i>).....	42
3.4.2 Konfigurasi IP Address	53
3.4.3 Penulisan Program.....	56
BAB IV PENGUJIAN SISTEM	61
4.1 Pengujian Autentifikasi.....	61
4.1.1 Tujuan Pengujian	61
4.1.2 Alat Pengujian.....	61

4.1.3 Prosedur Pengujian	62
4.1.4 Hasil Pengujian	62
4.2 Pengujian Serangan DoS.....	65
4.2.1 Tujuan	65
4.2.2 Alat Pengujian.....	65
4.2.3 Prosedur Pengujian	66
4.2.4 Hasil Pengujian	66
4.3 Pengujian Data Fuzzy	75
4.3.1 Tujuan	75
4.3.2 Alat Pengujian.....	75
4.3.3 Prosedur pengujian.....	75
4.3.4 Hasil Pengujian	76
4.4 Analisis Sistem	84
4.4.1 Pendeteksian Paket Normal.....	84
4.4.2 Pendeteksian Serangan Paket POD.....	87
4.4.3 Pendeteksian Serangan Paket UDP Flooding.....	89
4.4.4 Pendeteksian Serangan Paket TCP Flooding.....	91
4.4.5 Pendeteksian Paket Serangan <i>Syn-ACK</i>	93
4.4.6 Pendeteksian Paket HTTP	95
BAB V PENUTUP.....	98
5.1 Simpulan	98
5.2 Saran.....	99
DAFTAR PUSTAKA	xvi