

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	iv
DAFTAR TABEL.....	vii
DAFTAR GAMBAR	viii
DAFTAR SIMBOL.....	xi
DAFTAR LAMPIRAN.....	xii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah.....	3
1.3 Rumusan Masalah.....	3
1.4 Maksud dan Tujuan	3
1.5 Batasan Masalah	4
1.6 Metodologi Penelitian.....	5
1.6.1 Metode Pengumpulan Data	5
1.6.2 Metode Pengembangan Sistem	5
1.6.3 Kerangka Kerja Penelitian	6
1.7 Sistematika Penulisan	7
BAB 2 LANDASAN TEORI.....	9
2.1 Jaringan Komputer.....	9
2.2 Topologi.....	15
2.3 <i>Open System Interconnection (OSI)</i>	19
2.4 TCP/IP	21
2.5 IP Address.....	22
2.6 Port.....	23
2.7 Perangkat Jaringan.....	23

2.7.1	Hub.....	23
2.7.2	Repeater.....	24
2.7.3	Bridge.....	25
2.7.4	Switch.....	26
2.7.5	Router.....	26
2.8	Keamanan Jaringan Komputer.....	27
2.9	Model Serangan Keamanan Jaringan	28
2.10	Distributed Denial Of Service (DDoS).....	29
2.11	Malware.....	30
2.12	Intrusion Detection System (IDS)	30
2.12.1	Klasifikasi Intrusion Detection System (IDS)	30
2.12.2	Snort.....	31
2.12.3	Anomaly-Based	31
2.12.4	Signature Based	31
2.13	Intrusion Prevention System (IPS)	32
2.13.1	pfSense.....	33
2.14	Virtual Machine.....	33
2.14.1	Vmware Workstation.....	33
2.15	Sistem Operasi Komputer.....	34
2.15.1	Windows	34
2.15.2	Linux	35
BAB 3 ANALISIS DAN PERANCANGAN SISTEM	38
3.1	Analisis Sistem	38
3.2	Analisis Masalah.....	38
3.2.1	Analisis Sistem Yang Sedang Berjalan.....	39
3.2.2	Analisis Kebutuhan Informasi.....	40
3.2.3	Kebutuhan Data.....	41
3.2.4	Informasi Yang Dihasilkan	41
3.3	Analisis Kebutuhan Non-Fungsional.....	41
3.3.1	Analisis Kebutuhan Perangkat Keras	42
3.3.2	Analisis Kebutuhan Perangkat Lunak	42

3.3.3	Analisis Pengguna.....	43
3.4	Analisis Kebutuhan Fungsional	43
3.4.1	Diagram Alur Pengerjaan Sistem.....	44
3.4.2	Diagram Kinerja Snort	45
3.4.3	Kondisi Eksisting	46
3.4.4	Rancangan Usulan Sistem.....	47
3.5	Pengukuran Kinerja IDPS.....	48
3.5.1	Parameter Serangan.....	48
3.5.2	Parameter Komputasi	48
3.6	Parameter Keberhasilan Sistem	49
BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM.....		50
4.1	Instalasi PfSense	50
4.1.1	Instalasi Komputer IDPS.....	50
4.2	Konfigurasi PfSense Melalui webConfigurator PfSense.....	57
4.3	Konfigurasi Snort pada PfSense	61
4.4	Konfigurasi Notifikasi Telegram	69
4.5	Skenario Pengujian	76
4.6	Pengujian pada Sistem keamanan IDPS	76
4.6.1	Pengujian Port Scanning pada sistem IDPS	76
4.6.2	Pengujian DoS dan DDoS pada sistem IDPS	80
4.7	Kesimpulan Hasil Pengujian pada sistem keamanan IDPS dengan pfSense dan Snort.....	85
BAB 5 KESIMPULAN DAN SARAN.....		86
5.1	Kesimpulan	86
5.2	Saran	86
DAFTAR PUSTAKA		87