

DAFTAR ISI

SNORT SEBAGAI <i>INTRUSION DETECTION SYSTEM</i> DAN NOTIFIKASI MELALUI TELEGRAM	i
LEMBAR PENGESAHAN PEMBIMBING	ii
LEMBAR PENGESAHAN PENGUJI	iii
LEMBAR PERNYATAAN KEASLIAN HASIL TUGAS AKHIR	iv
HALAMAN PERSEMBAHAN	v
MOTTO	vi
KATA PENGANTAR	vii
SARI.....	ix
TAKARIR.....	x
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian.....	3
1.6 Metodologi Penelitian	3
1.7 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI	5
2.1 Snort	5
2.1.1 Mode Snort.....	5
2.1.2 Komponen Snort	7
2.2 <i>Intrusion Detection System</i>	10
2.2.1 Klasifikasi IDS	10
2.2.1 Metode Deteksi	11
2.3 <i>Notification Alert System</i>	13

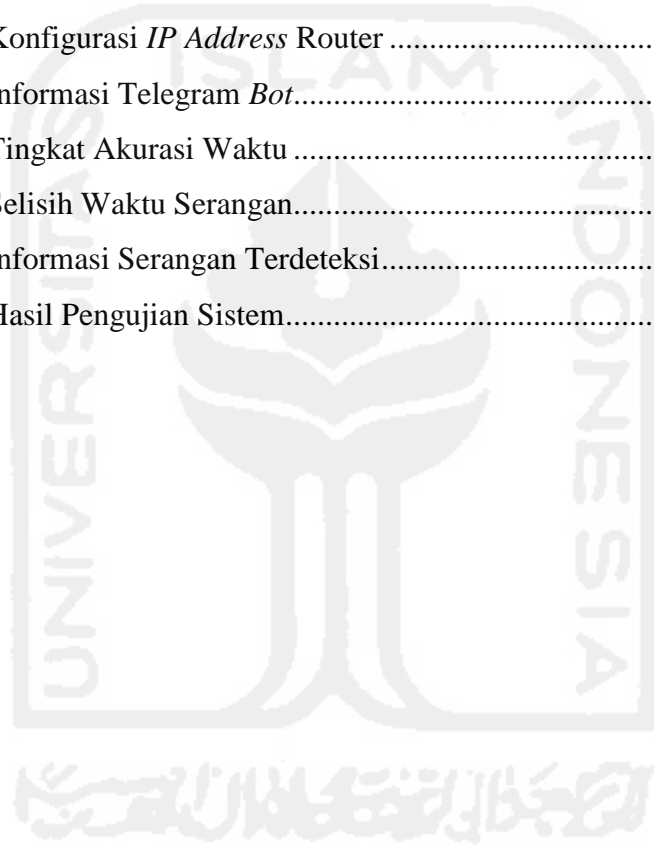
2.4	<i>Instant Messaging Telegram</i>	14
2.4.1	<i>Telegram Bot</i>	15
2.5	Kontribusi Penelitian	16
BAB III METODOLOGI		19
3.1	Analisis Kebutuhan Sistem	19
3.1.1	Kebutuhan Perangkat Keras	19
3.1.2	Kebutuhan Perangkat Lunak	20
3.2	Diagram Alur Penelitian	22
3.3	Gambaran Umum Sistem	24
3.4	Desain Sistem	25
3.4.1	Desain Antarmuka	26
3.5	Proses Kerja Sistem	31
3.5.1	Alur Deteksi Serangan	32
3.5.2	<i>Telegram Bot Token</i> dan ID Pengguna	33
3.5.3	Alur Kirim Notifikasi	34
3.6	Pengujian Sistem	35
3.6.1	Skenario Pengujian	36
3.7	Pengujian Sistem	36
3.7.1	Kuisisioner Pengujian	37
BAB IV HASIL DAN PEMBAHASAN		38
4.1	Implementasi Arsitektur Jaringan	38
4.1.1	Konfigurasi <i>IP Address IDS</i>	38
4.1.2	Konfigurasi <i>IP Address Server</i>	38
4.1.3	Konfigurasi <i>IP Address Attacker</i>	39
4.1.4	Konfigurasi Router	39
4.2	Implementasi Perangkat Lunak	39
4.2.1	Instalasi Aplikasi Pendukung	39
4.2.2	Instalasi dan Konfigurasi Snort	40
4.2.3	Instalasi dan Konfigurasi Barnyard2	41
4.2.4	Implementasi <i>Databse</i>	42
4.2.5	Implementasi <i>Rule Snort</i>	44

4.2.6	Hasil Implementasi Laporan <i>Web Based</i> Sistem	45
4.2.9	Implementasi Crontab	52
4.2.10	Hasil Pengujian Serangan	53
4.3	Hasil Akurasi Deteksi Intrusi	59
BAB V KESIMPULAN DAN SARAN.....		62
5.1	Kesimpulan.....	62
5.2	Saran	62
DAFTAR PUSTAKA		63
LAMPIRAN.....		64



DAFTAR TABEL

Tabel 3.1 Analisis Pengujian Serangan	36
Tabel 3.2 Analisis Pengujian Serangan	37
Tabel 4.1 Konfigurasi <i>IP Address</i> IDS.....	38
Tabel 4.2 Konfigurasi <i>IP Address Server</i>	38
Tabel 4.3 Konfigurasi <i>IP Address Attacker</i>	39
Tabel 4.4 Konfigurasi <i>IP Address Router</i>	39
Tabel 4.5 Informasi Telegram <i>Bot</i>	51
Tabel 4.6 Tingkat Akurasi Waktu	59
Tabel 4.7 Selisih Waktu Serangan.....	59
Tabel 4.8 Informasi Serangan Terdeteksi.....	60
Tabel 4.9 Hasil Pengujian Sistem.....	61



DAFTAR GAMBAR

Gambar 2.1 Komponen Snort (Kinal & Hajdarevic, 2013).....	9
Gambar 2.2 Arsitektur IDS (Anitha, 2011)	12
Gambar 2.3 Kontribusi Penelitian	17
Gambar 3.1 Diagram Alur Penelitian	22
Gambar 3.2 Implementasi IDS	24
Gambar 3.3 Topologi Jaringan	25
Gambar 3.4 Antarmuka Halaman <i>Login</i>	26
Gambar 3.5 Antarmuka Halaman <i>Dashboard</i>	27
Gambar 3.6 Aktifitas Laporan Insiden	27
Gambar 3.7 Menu Notifikasi Terkirim.....	28
Gambar 3.8 Antarmuka Menu Dokumen	29
Gambar 3.9 Antarmuka Menu Akun	29
Gambar 3.10 Antarmuka Notifikasi Telegram.....	30
Gambar 3.11 Dokumen Deteksi Intrusi.....	30
Gambar 3.12 Antarmuka BASE	31
Gambar 3.13 Diagram Use Case Sistem	31
Gambar 3.14 <i>Flowchart</i> Deteksi Serangan	32
Gambar 3.15 <i>Flowchart</i> Set Telegram <i>Bot Token</i>	33
Gambar 3.16 Alur Kirim Notifikasi	34
Gambar 3.17 Skenario Pengujian Sistem	35
Gambar 4.1 Implementasi Antarmuka BASE	44
Gambar 4.2 Halaman Beranda.....	46
Gambar 4.3 Halaman <i>Login</i>	46
Gambar 4.4 Halaman <i>Dashboard</i> Admin.....	47
Gambar 4.5 Halaman Aktifitas	47
Gambar 4.6 Halaman Notifikasi	48
Gambar 4.7 Menu Dokumen	48
Gambar 4.8 Menu Akun	49
Gambar 4.9 <i>Request</i> Telegram <i>Bot</i>	49

Gambar 4.10 Membuat Telegram <i>Bot</i>	50
Gambar 4.11 Mendapatkan <i>ID chat user</i> dan <i>group</i>	50
Gambar 4.12 Pengujian <i>Port Scanning</i>	53
Gambar 4.13 Deteksi <i>Port Scanning</i>	54
Gambar 4.14 Notifikasi <i>Port Scanning</i>	54
Gambar 4.15 Pengujian FTP Akses.....	54
Gambar 4.16 Deteksi FTP Akses	55
Gambar 4.17 Notifikasi FTP Akses.....	55
Gambar 4.18 Pengujian SSH <i>Brute Force</i>	55
Gambar 4.19 Deteksi SSH <i>Brute Force</i>	56
Gambar 4.20 Notifikasi SSH <i>Brute Force</i>	56
Gambar 4.21 Pengujian Ddos <i>Attack</i>	56
Gambar 4.22 Deteksi Ddos <i>Attack</i>	57
Gambar 4.23 Notifikasi Ddos <i>Attack</i>	57
Gambar 4.24 Informasi Serangan Terdeteksi	57
Gambar 4.25 Notifikasi Laporan Intrusi.....	58
Gambar 4.26 Laporan Insiden Terdeteksi	58
Gambar 4.27 Grafik Kuantitas Serangan.....	60