

DAFTAR ISI

LEMBAR PENGESAHAN	iii
PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR	v
ABSTRAK.....	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xii
BAB 1 PENDAHULUAN	13
1.1 Latar Belakang	13
1.2 Rumusan Masalah	15
1.3 Tujuan dan Manfaat	15
1.4 Batasan Masalah.....	16
1.5 Metodologi Penelitian	16
a. Identifikasi masalah	16
b. Studi literatur	17
c. Perancangan.....	17
d. Simulasi Penelitian	17
e. Pengujian	17
f. Analisa hasil	18
BAB 2 TINJAUAN PUSTAKA	19
2.1 Penelitian Terdahulu	19
2.2 Dasar Teori.....	20
2.2.1 <i>Intrusion Detection System (IDS)</i>	20
2.2.2 <i>Denial of Service</i>	21
2.2.3 <i>Distributed Denial of Service</i>	21
2.2.4 <i>Flood Data</i>	21
2.2.5 <i>Snort</i>	23
2.2.6 <i>Telegram</i>	24
BAB 3 METODOLOGI.....	25
3.1. Metode yang digunakan	25

3.2.	Alat dan Bahan Penelitian.....	25
3.3.	Prosedur Penelitian.....	27
3.3.1	Permasalahan Penelitian.....	27
3.3.2	Studi Literatur.....	28
3.3.3	Perancangan Arsitektur Jaringan.....	28
3.3.4	Identifikasi IDS.....	29
3.3.5	Menjalankan Simulasi Deteksi.....	31
3.3.6	Pengujian.....	31
3.3.7	Analisa Hasil.....	32
3.4.	Jadwal Pelaksanaan.....	32
BAB 4	HASIL DAN PEMBAHASAN.....	34
4.1	Install Aplikasi.....	34
4.2	Implementasi Serangan.....	35
4.3	Konfigurasi Snort.....	35
4.4	Instalasi dan Konfigurasi Barnyard2.....	37
4.5	Instalasi dan Konfigurasi Bot Telegram.....	41
4.6	Pengujian.....	46
4.6.1	Pengujian serangan.....	47
4.6.2	Hasil Pengujian.....	57
BAB 5	KESIMPULAN DAN SARAN.....	62
5.1	Kesimpulan.....	62
5.2	Saran.....	63
	DAFTAR PUSTAKA.....	64
	BIODATA PENULIS.....	66

DAFTAR GAMBAR

Gambar 2. 1 Bagian IDS	21
Gambar 3.1 Desain Simulasi Penelitian	25
Gambar 3. 2 Tahapan Penelitian	27
Gambar 3. 3 Arsitektur Jaringan	28
Gambar 3. 4 Snort Rules	29
Gambar 3. 5 Contoh Syntax Snort Rule	29
Gambar 3. 6 Simulasi sederhana arsitektur jaringan.....	31
Gambar 4.1 Instalasi Snort	34
Gambar 4.2 Versi Snort.....	35
Gambar 4.3 Topologi Serangan.....	35
Gambar 4.4 Tampilan file snort.conf	36
Gambar 4.5 Tampilan file parameter snort	37
Gambar 4.6 Penulisan rule snort	37
Gambar 4.7 Output database barnyard	39
Gambar 4.8 login mysql snort	39
Gambar 4.9 Memasukan Syntax mysql.....	40
Gambar 4.10 Database log snort pada mysql	40
Gambar 4.11 Diagram alur pembuatan bot telegram	41
Gambar 4.12 Request bot telegram	42
Gambar 4.13 Membuat bot telegram.....	42
Gambar 4.14 API Bot telegram.....	43
Gambar 4.15 Konfigurasi bot telegram.....	44
Gambar 4.16 Konfigurasi bot telegram.....	44
Gambar 4.17 Menjalankan bot telegram	44
Gambar 4.18 Menjalankan snort log.....	45
Gambar 4.19 Menjalan barnyard sebagai trigger	45
Gambar 4.20 Status barnyard telah berjalan	45
Gambar 4.21 Hasil test dari bot telegram.....	46
Gambar 4.22 Instalasi tools pembantui hping3 pada attacker.....	46
Gambar 4.23 scan port pada komputer target.....	47
Gambar 4.24 Simulasi penyerangan terhadap SYN port TCP	48

Gambar 4.25 Penyerangan TCP ke IP target.....	48
Gambar 4.26 Menjalankan snort pada mode IDS	49
Gambar 4.27 Deteksi SYN Flood pada port TCP	49
Gambar 4.28 Hasil pengujian pada periode 5 menit	50
Gambar 4. 29 Hasil pengujian pada periode 10 menit	50
Gambar 4. 30 Simulasi penyerangan terhadap UDP	51
Gambar 4.31 Percobaan penyerangan UDP ke IP Target	51
Gambar 4.32 Menjalankan snort pada mode IDS	52
Gambar 4.33 Hasil deteksi terhadap UDP.....	52
Gambar 4.34 Hasil pengujian pada periode 5 menit	52
Gambar 4.35 Hasil pengujian pada periode 10 menit	53
Gambar 4.36 Pengujian serangan ICMP Flood.....	54
Gambar 4.37 Proses percobaan penyerangan terhadap ICMP	54
Gambar 4.38 Menjalankan snort pada mode IDS	54
Gambar 4.39 Hasil deteksi terhadap ICMP.....	55
Gambar 4.40 Hasil pengujian pada periode 5 menit	55
Gambar 4.41 Hasil pengujian pada periode 10 menit	56
Gambar 4.42 Wireshark Capture.....	56
Gambar 4.43 Gambar Deteksi SYN TCP pada telegram	58
Gambar 4.44 Gambar Deteksi UDP pada telegram	58
Gambar 4.45 Gambar Deteksi ICMP pada telegram.....	59
Gambar 4.46 Hasil deteksi Snort Efisiensi pada percobaan pertama.....	60
Gambar 4.47 Hasil deteksi snort efisiensi pada percobaan kedua	61

DAFTAR TABEL

Tabel 3. 1 Spesifikasi Pengujian	26
Tabel 3. 2 Struktur Snort rule header	29
Tabel 3. 3 Parameter Penelitian	32
Tabel 3. 4 Jadwal Pelaksanaan	33
Tabel 4.1 Informasi bot telegram	43
Tabel 4.2 Skenario Penyerangan	47
Tabel 4.3 Hasil pengujian ke telegram	57
Tabel 4.4 Hasil pengujian sistem	58
Tabel 4.5 Hasil akurasi pengujian	59