

DAFTAR ISI

1. HALAMAN DEPAN.....	i
2. HALAMAN DEPAN II.....	ii
3. PENGESAHAN.....	iii
4. PENGESAHAN PENGUJI.....	iv
5. PERNYATAAN KEASLIAN.....	v
6. PERSEMBAHAN.....	vi
7. MOTTO.....	vii
8. PENGANTAR.....	viii
9. DAFTAR ISI.....	ix
10. DAFTAR TABEL.....	xi
11. DAFTAR GAMBAR.....	xi
12. ABSTRAK.....	xiii
13. BAB I PENDAHULUAN	
13.1. Latar Belakang Masalah.....	1
13.2. Perumusan Masalah.....	4
13.3. Tujuan Penelitian.....	4
13.4. Manfaat Penelitian.....	4
13.5. Metodologi Penelitian.....	5
13.6. Batasan Penelitian.....	5
13.7. Sistematika Penulisan.....	6
14. BAB II TINJAUAN PUSTAKA	
2.1. Kajian Kepustakaan.....	7
a. Masalah Penelitian.....	7
b. Deteksi Abnormal.....	7
2.2. Dasar Teori.....	10
a. <i>Log</i>	10
b. VSFTP.....	10
c. <i>Denial of Service</i>	11
d. <i>Data Mining</i>	12
e. <i>Clustering</i>	13
f. Algoritma <i>K-Means</i>	15
g. Kedekatan (<i>Density</i>).....	15
h. Jarak.....	16
i. Validasi <i>Cluster</i>	16
j. TCP/IP.....	18
k. Proses <i>Three-Way Handshake</i>	24
l. Klasifikasi Serangan dalam Jaringan Komputer.....	26
m. Deteksi dengan <i>IP Header</i>	27
n. Deteksi Jaringan Abnormal.....	27
15. BAB III METODOLOGI PENELITIAN	

3.1. Perancangan Skenario.....	28
3.1.1. Skenario Topologi Jaringan.....	28
3.1.2. Skenario <i>Client-Server</i>	29
3.1.3. Skenario Serangan <i>DoS</i>	30
3.1.4. Skenario Analisis.....	31
3.1.5. Skenario <i>Data Mining</i>	32
3.1.6. Skenario <i>Clustering</i>	33
3.1.7. Skenario Sistem.....	33
3.2. Penerapan Skenario	37
3.2.1. Penerapan <i>Log Capturing</i>	37
3.2.2. Penerapan <i>Log Extraction</i>	39
3.2.3. Penerapan Ekstraksi Fitur	41
3.2.4. Penerapan <i>Clustering</i>	45
3.2.5. <i>Davies-Bouldin Index</i>	49
3.2.6. Penerapan Sistem.....	50
16. BAB IV HASIL DAN PEMBAHASAN	
4.1. Analisis <i>Log</i> Menggunakan <i>Density K-Means</i>	55
a. <i>Log</i>	55
b. Klasifikasi Tingkat Bahaya.....	57
c. <i>Density K-Means</i>	57
d. <i>Davies-Bouldin Index</i>	57
4.2. Hasil <i>Clustering Density K-Means</i>	59
4.3. Skenario Pengujian Serangan <i>DoS</i>	60
4.4. Verifikasi log untuk <i>DoS</i> Port 21 (FTP) dengan LOIC.....	64
4.5. Verifikasi log untuk <i>DoS</i> dengan FTP Bruteforce	65
17. BAB V PENUTUP	
5.1. Kesimpulan.....	66
5.2. Saran.....	66

DAFTAR PUSTAKA

DAFTAR TABEL

Tabel 2.1.	Masalah Penelitian	8
Tabel 2.2.	Tinjauan Pustaka	9
Tabel 2.3.	Klasifikasi Serangan Jaringan Komputer	26
Tabel 3.1a.	<i>Length</i>	42
Tabel 3.1b.	<i>Tcplength</i>	43
Tabel 3.2.	Frekuensi <i>Length & TCPlength</i>	44
Tabel 3.3.	Perhitungan Jarak iterasi ke-1	47
Tabel 3.4.	Rata-rata pada <i>centroid</i> yang sama	48
Tabel 3.5.	Jumlah data pada <i>centroid</i>	48
Tabel 3.6.	<i>Cluster</i> yang diikuti.....	50
Tabel 3.7.	Data pada C_1, C_2, C_3	51
Tabel 3.8.	<i>Centroid</i> hasil proses <i>clustering</i>	51
Tabel 3.9.	<i>SSW</i>	52
Tabel 3.10.	<i>SSB</i>	52
Tabel 3.11.	<i>R & DBI</i>	52
Tabel 4.1.	Klasifikasi Tingkat Bahaya	57
Tabel 4.2.	Hasil Klasifikasi Tingkat Bahaya.....	60

DAFTAR GAMBAR

Gambar 1.1.	Skema Analisis Serangan	5
Gambar 2.1.	<i>DoS</i>	11
Gambar 2.2.	<i>TCP SYN FLOODING</i>	12
Gambar 2.3.	<i>Proses KDD</i>	12
Gambar 2.4.	<i>Clustering</i>	14
Gambar 2.5.	Algoritma <i>K-Means</i>	15
Gambar 2.6.	Kohesi & Separasi	17
Gambar 2.7.	Datagram TCP	19
Gambar 2.8.	Datagram IP	22
Gambar 2.9.	<i>Three-Way Handshake</i>	24
Gambar 2.10.	Luaran TCPDUMP	24
Gambar 2.11.	<i>IP Header</i>	27
Gambar 3.1.	Skenario Topologi Jaringan	28
Gambar 3.2.	Skenario <i>Client-Server</i>	30
Gambar 3.3.	Serangan <i>DoS</i>	31
Gambar 3.4.	Skenario Analisis	31
Gambar 3.5.	Skenario Ekstraksi Data Jaringan	33
Gambar 3.6.	Skenario <i>Clustering</i>	34
Gambar 3.7.	<i>Flowchart Density K-Means</i>	36
Gambar 3.8.	Rancangan Sistem <i>Density K-Means</i>	37
Gambar 3.9.	Potongan perintah TCPDUMP	38

Gambar	3.10.	Potongan Berkas <i>Log</i>	38
Gambar	3.11.	Skrip untuk Ekstraksi Data	39
Gambar	3.12.	Struktur Tabel	40
Gambar	3.13a.	<i>log</i>	40
Gambar	3.13b.	<i>log</i>	41
Gambar	3.14a	Fitur <i>length</i>	42
Gambar	3.14b	Fitur <i>tcplength</i>	42
Gambar	3.15.	Tampilan Antarmuka	53
Gambar	4.1.	Skrip <i>Regex</i>	56
Gambar	4.2.	Potongan Basisdata <i>log</i>	57
Gambar	4.3.	Topologi Jaringan	61
Gambar	4.4.	LOIC	63
Gambar	4.5.	FTP <i>Bruteforce</i>	64
Gambar	4.6.	Verifikasi Log menggunakan LOIC.....	64
Gambar	4.7.	Verifikasi Log menggunakan FTP <i>Bruteforce</i>	65

