

DAFTAR GAMBAR

Gambar 2.1 Database <i>Malware</i> pada Maltrail.....	7
Gambar 2.2 Fitur Fail2Ban.....	8
Gambar 2.3 Struktur Organisasi Diskominfo Sumedang	10
Gambar 3.1 Gambaran Sistem Saat ini.....	12
Gambar 3.2 Gambaran Sistem Usulan	14
Gambar 3.3 Topologi Sistem.....	15
Gambar 3.4 Penerapan Skema Topologi Jaringan Diskominfo Sumedang	16
Gambar 3.5 Flowchart Sistem	18
Gambar 3.6 Use Case Diagram Sistem Maltrail	21
Gambar 4.1 Perintah Instalasi <i>Software</i> Maltrail	28
Gambar 4.2 Konfigurasi Sistem Maltrail.....	29
Gambar 4.3 Instalasi dan Konfigurasi Fail2Ban.....	30
Gambar 4.4 Kode Program Deklarasi <i>regex-script</i> pada Fail2Ban.....	31
Gambar 4.5 Kode Program Deklarasi pelaporan <i>real-time</i> Fail2Ban ke Telegram	32
Gambar 4.6 Kode Program Deklarasi <i>variable konfigurasi</i>	32
Gambar 4.7 Tampilan Dashboard Sistem Maltrail.....	33
Gambar 4.8 Grafik Sistem Maltrail.....	34
Gambar 4.9 Rules Pengintegrasian Fail2Ban ke Telegram	35
Gambar 4.10 Laporan Status Sistem Ryzenware ke Telegram Administrator	36
Gambar 4.11 Hasil Uji Coba Lima Situs yang terindikasi <i>Malware</i>	38
Gambar 4.12 Hasil <i>Banned</i> Alamat IP oleh Fail2Ban.....	39
Gambar 4.13 Hasil Laporan Blocking oleh Fail2Ban ke Telegram Administrator	40
Gambar 4.14 Hasil Tampilan <i>Log</i> Rekapitulasi <i>Malware</i>	41
Gambar 4.15 Hasil Serangan <i>DDos Attack</i>	42
Gambar 4.16 Hasil <i>Scanning Port</i>	43
Gambar 4.17 Grafik Tingkat Ancaman <i>Scanning Port</i>	43
Gambar 4.18 Hasil Serangan <i>Syn Flooding</i>	44
Gambar 4.19 Wireshark untuk menangkap paket data pada server	45
Gambar 4.20 Wireshark menangkap paket data enkripsi berupa <i>malware</i>	45

Gambar 4.21 Grafik throughput pada serangan <i>malware</i> sinkhole conficker.....	48
Gambar 4.22 Grafik throughput pada serangan <i>malware</i> andromeda.....	49
Gambar 4.23 Grafik throughput pada serangan <i>malware</i> sinkhole shadowserver	49
Gambar 4.21 Grafik throughput pada serangan <i>malware</i> sinkhole response.....	50