DAFTAR ISI

HALAMAN SAMPUL i
LEMBAR PENGESAHAN iii
PERNYATAAN BEBAS PLAGIASI iv
KATA PENGANTAR v
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xiii
INTISARI xv
BAB I PENDAHULUAN 19
1.1. Latar Belakang 19
1.2. Rumusan Masalah 21
1.3. Batasan Masalah 21
1.4. Tujuan Penelitian 22
1.5. Manfaat Penelitian 22
1.6. Sistematika Penulisan 23
BAB II TINJAUAN PUSTAKA 24
2.1. *Intrusion Detection System* 27
2.1.1. Berdasarkan Input Data 27
2.1.2. Berdasarkan Pengolahan Data 28
2.2. *Intrusion Prevention System* 29
2.3. *Intrusion Detection and Prevention System* 29
2.4. Suricata 30
2.5. Promiscuous 31

2.6. Inline 32
2.7. Elasticsearch 32
2.8. Kibana 33
2.9. Filebeat 33
2.10. Hydra 33
2.11. Nmap 33
2.12. Hping3 34
2.13. Hipotesis 34
BAB III METODE PENELITIAN 35
3.1. Bahan Penelitian 35
3.2. Alat Penelitian 38
3.3. Tahap Penelitian 39
3.4. Perancangan Sistem dan Instalasi 41
3.4.1. Perancangan Topologi 41
3.5. Instalasi dan Konfigurasi Server 44
3.5.1. Instalasi Suricata 44
3.5.2. Instalasi Trafr 48
3.5.3. Konfigurasi Bot Telegram dan Instalasi Swatch 49
3.5.4. Instalasi Elasticsearch, Kibana, dan Filebeat 51
3.6. Tahap Pengujian 53
3.6.1. *Dashboard* Kibana 53
3.6.2. Percobaan Serangan 55
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 62
4.1. Hasil dan Analisis Pengujian Tingkat Keberhasilan Suricata 62
4.1.1. Suricata Mode Promiscuous 62

4.1.2. Suricata Mode Inline 66
4.2. Hasil dan Analisis Pengujian *Response Time* 70
4.2.1. Suricata Mode Promiscuous 71
4.2.2. Suricata Mode Inline 77
4.3. Hasil dan Analisis Penggunaan *Resources* 85
4.3.1. Suricata Mode Promiscuous 86
4.3.2. Suricata Mode Inline 87
4.4. Notifikasi Telegram 89
BAB V 90
PENUTUP 90
5.1. Kesimpulan 90
5.2. Saran 91
DAFTAR PUSTAKA 92