

DAFTAR ISI

HALAMAN JUDUL	ii
HALAMAN PENGESAHAN	iii
PERNYATAAN KEASLIAN PENELITIAN	iv
KATA PENGANTAR	v
DAFTAR ISI	ix
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiv
INTISARI	xv
ABSTRACT	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	5
1.6 Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI	7
2.1 Tinjauan Pustaka	7
2.2 Landasan Teori	20
2.2.1 <i>Internet of Things (IoT)</i>	20
2.2.2 <i>SYN Flood Attack</i>	21
2.2.3 <i>Secure Shell (SSH)</i>	23
2.2.4 Raspberry Pi	24
2.2.5 Iptables	25
2.2.6 Ipset	32
2.2.7 <i>Hping3</i>	33
2.2.8 <i>Docker dan Docker Compose</i>	33
2.2.9 <i>ELK Stack</i>	34
2.2.10 Filebeat	36
2.2.11 <i>Rsyslog</i>	36
2.2.12 <i>Ksoftirqd</i>	37
2.3 Hipotesis	38
BAB III METODE PENELITIAN	39
3.1 Bahan	39



3.2	Peralatan.....	40
3.3	Tahapan Penelitian.....	42
3.4	Rancangan Sistem.....	44
3.4.1	Topologi Jaringan.....	44
3.4.2	Alur Pemrosesan <i>Logs</i>	45
3.4.3	Konfigurasi Raspberry Pi.....	46
3.4.4	Konfigurasi WAP Raspberry Pi.....	50
3.4.5	Aturan Iptables.....	54
3.4.6	Skenario Pengujian.....	60
3.4.7	Konfigurasi <i>ELK Stack</i> dan Filebeat.....	65
3.4.8	Konfigurasi Rsyslog.....	68
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....		72
4.1	Hasil Pembangunan <i>ELK Server</i>	72
4.2	Hasil Pengujian Aturan UNRECOGDVC.....	76
4.3	Hasil Pengujian Aturan SSHATTACK.....	80
4.4	Hasil Pengujian Aturan SYN Flood.....	84
BAB V PENUTUP.....		100
5.1	Kesimpulan.....	100
5.2	Saran.....	101
DAFTAR PUSTAKA.....		104
LAMPIRAN.....		108