

DAFTAR ISI

LEMBAR PENGESAHAN BUKU CAPSTONE DESIGN	i
LEMBAR PERNYATAAN ORISINALITAS	ii
TIMELINE REVISI DOKUMEN	v
ABSTRAK.....	x
ABSTRACT.....	xi
KATA PENGANTAR	xii
UCAPAN TERIMA KASIH.....	xiii
DAFTAR ISI.....	xiv
DAFTAR GAMBAR.....	xix
DAFTAR TABEL.....	xxii
DAFTAR SINGKATAN	xxiv
BAB 1	
USULAN GAGASAN DAN PEMILIHAN TOPIK	1
1.1. Latar Belakang Masalah	1
1.2. Informasi Pendukung Masalah	2
1.2.1. Serangan Malware Terhadap Jaringan dan IoT	2
1.2.2. Intrusion Detection System (IDS) dengan Raspberry Pi	3
1.2.3. Integrasi Sistem Notifikasi Real-Time.....	3
1.2.4. Pemilihan Raspberry Pi 5 Sebagai Platform IDS	3
1.3. Analisis Umum	5
1.3.1. Aspek Teknis	5
1.3.2. Aspek Ekonomi.....	5
1.3.3. Aspek Hukum dan Regulasi.....	6
1.3.4. Aspek Keberlanjutan.....	6
1.3.5. Aspek Lingkungan	6
1.4. Kebutuhan yang Harus Dipenuhi.....	6
1.5. Solusi Sistem yang Diusulkan	8
1.5.1. Karakteristik Produk	8

1.5.2. Analisa Solusi yang Ada	8
1.6. Kesimpulan	15
BAB 2	
SPESIFIKASI	16
2.1. Dasar Penentuan Spesifikasi	16
2.1.1. Kebutuhan User	17
2.1.2. Peraturan Pemerintah	18
2.1.3. Standar Industri	19
2.1.4. Standar Teknologi	20
2.1.5. Data dari Penelitian dan Literatur Ilmiah	20
2.1.6. Threat Modeling STRIDE pada IoT	21
2.2. Batasan dan Spesifikasi	22
2.2.1. Spesifikasi Kinerja Sistem	23
2.2.2. Indikator Performa Akurasi Deteksi	27
2.3. Verifikasi Spesifikasi	27
2.3.1. Spesifikasi 1: Pengujian Raspberry Pi 5 Dalam Memenuhi Kebutuhan Penggunaan IDS	27
2.3.2. Spesifikasi 2: Pengujian Kompatibilitas Aplikasi Dengan Software	28
2.3.3. Spesifikasi 3: pengujian akurasi deteksi ancaman snort	28
2.3.4. Spesifikasi 4: Pengujian ruleset snort yang digunakan	29
2.3.5. Spesifikasi 5: Verifikasi sistem notifikasi telegram pada IDS	30
2.3.6. Spesifikasi 6: Verifikasi Logging dan Penyimpanan IDS	31
2.4. Kesimpulan	31
BAB 3	
DESAIN RANCANGAN SOLUSI	33
3.1. Alternatif Usulan Solusi	33
3.1.1. Alternatif Solusi IDS	33
3.1.2. Alternatif Solusi pemilihan Case	36
3.1.3. Alternatif Solusi pemilihan Sistem Pendingin	37
3.1.4. Alternatif Solusi Sistem Notifikasi Intrusi	39

3.1.5. Alternatif Solusi pemilihan Sistem Operasi.....	41
3.1.6. Alternatif Solusi pemilihan Sistem Penyimpanan Data.....	43
3.2. Analisis dan Pemilihan Solusi	45
3.2.1. Parameter yang Digunakan untuk Menetapkan Solusi	45
3.2.2. Analisis Pemilihan Perangkat IDS.....	47
3.2.3. Analisis Pemilihan Casing Perangkat	48
3.2.4. Analisis Pemilihan Sistem Pendingin	49
3.2.5. Analisis Pemilihan Sistem Notifikasi Intrusi	50
3.2.6. Analisis Pemilihan Sistem Operasi.....	51
3.2.7. Analisis Pemilihan Memori Penyimpanan Data	52
3.2.8. Hasil Pemilihan Solusi.....	53
3.3. Desain Solusi Terpilih.....	55
3.3.1. Diagram Blok Sistem.....	55
3.3.2. Flowchart Sistem	56
3.3.3. Flowchart IDS.....	58
3.3.4. Flowchart Sistem Notifikasi	59
3.3.5. Use Case Diagram.....	61
3.3.6. DFD level 0.....	62
3.3.7. DFD level 1	63
3.3.8. DFD level 2.....	64
3.3.9. Perhitungan Biaya konsumsi daya Listrik pada IoT Network Security IDS	65
3.3.10. Modul Raspberry Pi 5	66
3.3.11. Threat Modeling STRIDE.....	70
3.4. Jadwal dan Anggaran.....	71
3.4.1. Jadwal Pengerjaan.....	71
3.4.2. Anggaran Biaya	72
3.5. Kesimpulan	73
BAB 4	
IMPLEMENTASI.....	74

4.1. Deskripsi Umum Implementasi	74
4.1.1. Raspberry Pi 5	76
4.1.2. Snort3	77
4.1.3. Bot Telegram	77
4.1.4. Log alert_fast Snort 3.0.....	78
4.1.5. Push/Pull GitHub	79
4.2. Detail Implementasi	80
4.2.1. Konfigurasi Raspberry pi 5	80
4.2.2. Konfigurasi Snort3	86
4.2.3. Konfigurasi Notifikasi Telegram	94
4.2.4. Konfigurasi Github backup dalam logging.....	100
4.3. Prosedur Pengoperasian	106
4.3.1. Pengoperasian Pendeteksian serangan	106
4.3.2. Pengoperasian notifikasi dan log	107
4.4. Kesimpulan	111
BAB 5	
PENGUJIAN DAN KESIMPULAN	112
5.1. Skenario Umum Pengujian	112
5.1.1. Skenario Pengujian Stabilitas dan Kinerja CPU	112
5.1.2. Skenario Pengujian Memori	112
5.1.3. Skenario Pengujian I/O Storage	113
5.1.4. Skenario Pengujian Konektivitas Ethernet, Wi-Fi dan Mode Bridge	113
5.1.5. Skenario Pengujian Fungsionalitas Sistem Snort	114
5.1.6. Skenario Pengujian Deteksi Serangan	114
5.1.7. Skenario Pengujian False Positive Rate Rules IDS	116
5.1.8. Skenario Pengujian Mode Inline IPS	116
5.1.9. Skenario Pengujian Sistem Notifikasi Telegram	116
5.1.10. Skenario Pengujian Log	118
5.2. Detail Pengujian.....	118

5.2.1. Pengujian Stabilitas dan Kinerja CPU	118
5.2.2. Pengujian Memori.....	119
5.2.3. Pengujian I/O Storage	121
5.2.4. Pengujian Konektivitas Ethernet, Wi-Fi dan Mode Bridge	123
5.2.5. Pengujian Pengujian Fungsionalitas Sistem Snort.....	126
5.2.6. Pengujian Deteksi Serangan	128
5.2.7. Pengujian False Positive Rate Rules IDS	131
5.2.8. Pengujian Mode IPS Snort.....	132
5.2.9. Pengujian Notifikasi Telegram	133
5.2.10. Pengujian Log	139
5.3. Analisa Hasil Pengujian.....	141
5.3.1 Analisis Device Raspberry Pi 5 Keseluruhan	141
5.3.2. Analisis Program Snort.....	143
5.3.3. Analisis Notifikasi dan Logging	147
5.4. Kesimpulan	150
DAFTAR PUSTAKA	151
LAMPIRAN CD-1	157
LAMPIRAN CD-2.....	158
LAMPIRAN CD-3.....	159
LAMPIRAN CD-4.....	160
LAMPIRAN CD-5.....	161