

DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS	ii
LEMBAR PENGESAHAN	iii
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiii
DAFTAR SINGKATAN.....	xiv
DAFTAR ISTILAH	xv
BAB I PENDAHULUAN.....	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	2
I.3 Tujuan Penelitian	2
I.4 Manfaat Penelitian	3
I.5 Batasan Masalah.....	3
BAB II TINJAUAN PUSTAKA.....	4
II.1 <i>Software Defined Network (SDN)</i>	4
II.1.1 <i>Application Plane</i>	5
II.1.2 <i>Control Plane</i>	5
II.1.3 <i>Data Plane</i>	6
II.1.4 <i>Southbound API</i>	6
II.1.5 <i>Northbound API</i>	7
II.2 OpenFlow	7

II.3 Controller	7
II.4 Mininet.....	8
II.5 Distributed Denial of Service (DDoS).....	9
II.6 Scapy.....	9
II.7. Shannon <i>Entropy</i>	9
II.8 <i>PPDIOO</i>	10
II.8.1 <i>Prepare</i>	10
II.8.2 <i>Plan</i>	11
II.8.3. <i>Design</i>	11
II.8.4. <i>Implement</i>	11
II.9 Penelitian Terdahulu	11
BAB III METODE PENELITIAN	13
III.1 Pengembangan Model Konseptual	13
III.2 Sistematika Penelitian	14
III.2.1 Tahap Awal (<i>Prepare Stage</i>)	15
III.2.2 Tahap Perencanaan (Plan Stage).....	15
III.2.3 Tahap Perancangan (<i>Design Stage</i>)	15
III.2.4 Tahap Implementasi (<i>Implement Stage</i>)	15
III.2.5 Tahap Analisis Pasca-Implementasi (<i>Post-implementation Analysis Stage</i>)	16
III.3 Alasan Pemilihan Metode	16
BAB IV PERANCANGAN PENELITIAN.....	18
IV.1 PPDIOO	18
IV.1.1 Prepare.....	18
IV.1.2 Plan	21
IV.1.3 Design.....	23

BAB V PENGUJIAN DAN HASIL	30
V.1 Implementasi	30
V.2 Pengujian Skenario	30
V.2.1 Pengujian Konektivitas Sebelum Serangan	30
V.2.2 Buka Terminal XTerm	32
V.2.3 Pengujian <i>Normal Traffic</i>	32
V.2.4 Pengujian Skenario Serangan <i>DDoS</i>	34
V.3 Analisis Data Serangan	51
BAB VI KESIMPULAN DAN SARAN	56
VI.1 Kesimpulan	56
VI.2 Saran	57
DAFTAR PUSTAKA	58
LAMPIRAN A – <i>SCRIPT</i> TOPOLOGI SDN	59
LAMPIRAN B – <i>SCRIPT</i> SERANGAN <i>DDOS</i>	61
LAMPIRAN C – <i>SCRIPT SHANNON ENTROPY CALCULATOR</i>	63
LAMPIRAN D – <i>SCRIPT</i> DETEKSI MENGGUNAKAN <i>SHANNON ENTROPY</i>	65