

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR	v
KATA PERSEMBAHAN	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR ISTILAH	xiii
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	2
I.3 Tujuan Penelitian	3
I.4 Batasan Penelitian	3
I.5 Manfaat Penelitian	4
BAB II LANDASAN TEORI	5
II.1 Keamanan Siber	5
II.2 Jaringan Komputer Konvensional.....	5
<i>II.3 Software-Defined Networking (SDN)</i>	5
<i>II.4 Mininet</i>	5
<i>II.5 Distributed Denial-of-Service (DDoS)</i>	6
<i>II.6 HTTP Flood</i>	6
<i>II.7 Virtual Machine</i>	6

II.8	<i>Rate Limiting</i>	7
II.9	<i>Ryu Controller</i>	7
II.10	<i>Wireshark</i>	7
II.11	<i>Support Vector Machine (SVM)</i>	7
II.12	<i>Confusion Matrix</i>	8
II.13	Metode PPDIOO.....	8
II.14	Penelitian Terdahulu.....	8
BAB III	METODE PENYELESAIAN MASALAH.....	12
III.1	Kerangka Berpikir.....	12
III.2	Sistematika Penyelesaian Masalah.....	13
III.3	Pengumpulan data.....	17
III.4	Pengolahan Data atau Pengembangan Produk / Artifak.....	19
III.5	Metode Evaluasi.....	20
III.6	Alasan Pemilihan Metode.....	21
BAB IV	PENYELESAIAN MASALAH.....	24
IV.1	Alur Perancangan.....	24
IV.1.1	<i>Prepare</i>	24
IV.1.2	<i>Plan</i>	29
IV.1.3	<i>Design</i>	30
BAB V	VALIDASI, ANALISIS HASIL, DAN IMPLIKASI.....	39
V.1	Pengujian Skenario 1.....	39
V.1.1	Hasil Pengujian.....	39
V.1.2	Analisis Pengujian Skenario 1.....	48
V.2	Pengujian skenario 2.....	49
V.2.1	Analisis Pengujian Skenario 2.....	58
V.3	Pengujian Skenario 3.....	59

V.3.1	Analisis Pengujian Skenario 3	70
V.4	Analisis Perbandingan Hasil Pengujian	71
V.4.1	Perbandingan Kinerja Jaringan	71
V.4.2	Perbandingan Kinerja Deteksi dan Mitigasi	72
V.4.3	Hasil Utama dan Temuan Analisis.....	73
BAB VI	KESIMPULAN DAN SARAN.....	75
VI.1	Kesimpulan	75
VI.2	Saran.....	76
Daftar Pustaka		77
Lampiran		79