

DAFTAR ISI

LEMBAR PERNYATAAN ORISINILITAS	i
LEMBAR PENGESAHAN	ii
ABSTRAK	iii
ABSTRACT	iv
UCAPAN TERIMA KASIH	v
KATA PENGANTAR	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR LAMPIRAN	xiii
DAFTAR SINGKATAN	xiv
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian	2
1.4 Manfaat Penelitian	3
1.5 Batasan Masalah	3
1.6 Sistematika Penulisan	3
BAB 2 TINJAUAN PUSTAKA	5
2.1 <i>Software Defined Network (SDN)</i>	5
2.2 <i>OpenFlow</i>	7
2.3 <i>Controller</i>	8
2.3.1 Ryu Controller	9
2.4 Mininet	10

2.5	SDN Vulnerability.....	11
2.6	Relay Attack.....	12
2.7	Pengujian QoS Dengan Standar TIPHON	13
2.7.1	Latency (Delay).....	14
2.8	IP Spoofing.....	14
2.9	Scapy	15
2.10	PPDIOO.....	15
2.10.1	Prepare (persiapan)	15
2.10.2	Plan (perencanaan)	16
2.10.3	Design (perancangan)	16
2.10.4	Implement (implementasi).....	16
2.10.5	Operate (pengoperasian).....	16
2.10.6	Optimize (optimasi).....	16
2.11	Penelitian Terdahulu	17
BAB 3	METODOLOGI PENELITIAN	19
3.1	Model Konseptual	19
3.2	Sistematika Penelitian	20
3.2.1	Tahap Awal.....	21
3.2.2	Tahap Implementasi (Eksperimen Simulasi Penyerangan)	21
3.2.3	Tahap Akhir (Dokumentasi Laporan Simulasi).....	21
3.3	Alasan Pemilihan Metode	22
BAB 4	PERANCANGAN SISTEM DAN SKENARIO PENGUJIAN	24
4.1	Alur Perancangan dengan PPDIOO	24
4.1.1	Prepare	24
4.1.2	Plan.....	27
4.1.3	Design	30

BAB 5	PENGUJIAN DAN HASIL	36
5.1	Simulasi Serangan	36
5.2	Pengujian Skenario Serangan	36
5.2.1	Pengujian Konektivitas Sebelum Serangan	36
5.2.2	Pengujian Serangan <i>Relay Attack (Fake Link)</i>	38
5.2.3	Pengujian Serangan <i>IP Spoofing</i>	42
5.3	Analisis Data Normal & Data Serangan	46
5.3.1	Analisis Data Serangan Pada 10.1.1.3 (<i>Host3</i>)	47
5.3.2	Analisis Data Serangan Pada 10.1.1.5 (<i>Host5</i>)	52
BAB 6	KESIMPULAN DAN SARAN	58
6.1	Kesimpulan.....	58
6.2	Saran.....	59
DAFTAR PUSTAKA	60
LAMPIRAN	62