

DAFTAR ISI

HALAMAN JUDUL	ii
LEMBAR PENGESAHAN	iii
PERNYATAAN KEASLIAN PENELITIAN	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
INTISARI	xii
ABSTRACT	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	2
1.6 Sistematika Penelitian	2
BAB II LANDASAN TEORI	4
2.1 Lingkup Tinjauan Pustaka	4
2.2 Landasan Teori	8
2.2.1 <i>Software Define Network (SDN)</i>	8
2.2.2 <i>Denial of Service (DoS)</i>	10
2.2.3 <i>Intrusion Detection System (IDS)</i>	10
2.2.4 Snort	11
2.2.5 Iptables	12
2.2.6 Ubuntu	13
2.2.7 Kali Linux	14
2.2.8 Metasploit Framework	14
2.2.9 Hping3	15
2.2.10 Slowhttptest	15
2.2.11 Slowloris	16
2.2.12 LOIC	16
2.2.13 Router Mikrotik	16
2.3 Hipotesis	17

BAB III METODE PENELITIAN	18
3.1 Alat dan Bahan.....	18
3.1.1 Perangkat Keras.....	18
3.1.2 Perangkat Lunak.....	19
3.2 Prosedur Penelitian	19
3.3 Rancangan Penelitian.....	21
3.3.1 Topologi Jaringan.....	21
3.3.2 Desain Sistem	22
3.4 Instalasi dan Konfigurasi	23
3.4.1 Instalasi dan Konfigurasi Ubuntu 18.04.6 LTS.....	23
3.4.2 Instalasi dan Konfigurasi ONOS	24
3.4.3 Instalasi dan Konfigurasi Kali Linux.....	26
3.4.4 Instalasi dan Konfigurasi Snort	28
3.4.5 Konfigurasi Iptables	32
3.4.6 Konfigurasi Mikrotik dan SDN	36
3.5 Percobaan Serangan.....	45
3.5.1 Penyerangan <i>Port</i> 1099	45
3.5.2 Penyerangan <i>Port</i> 9876	47
3.5.3 Penyerangan <i>Port</i> 8181	48
3.6 Skenario Pengujian	49
BAB IV HASIL DAN PEMBAHASAN	50
4.1 Penerapan <i>Software Defined Network</i>	50
4.2 Analisis Kerentanan Sistem	50
4.3 Pengujian Penerapan Snort IDS.....	54
4.4 Pengujian Penerapan Iptables	58
BAB V KESIMPULAN.....	63
5.1 Kesimpulan	63
5.2 Saran	63
DAFTAR PUSTAKA.....	64
LAMPIRAN	66