DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS ii
LEMBAR PENGESAHAN iii
ABSTRAK iv
ABSTRACT v
UCAPAN TERIMA KASIH vi
KATA PENGANTAR vii
DAFTAR ISI viii
DAFTAR GAMBAR x
DAFTAR TABEL xi
DAFTAR ISTILAH xii
DAFTAR SINGKATAN xiii
BAB I 1
PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Tujuan dan Manfaat 2
1.3 Perumusan Masalah 2
1.4 Batasan Masalah 2
1.5 Metode Penelitian 3
BAB II TINJAUAN PUSTAKA 5
2.1 *Transmission Control Protocol (TCP)* 5
2.2 *Denial of Service (DOS)* dan *Distributed Denial of Service(DDOS)* 6
2.2.1 SYN Flood Attack 7
2.3 Host-Based Intrusion Prevention System(HIPS) 8
2.4 Snort 9
2.4.1 General Rule Options 11
2.5 Wireshark 13
2.6 Zabbix 14
BAB III perancangan sistem 15
3.1 Desain Sistem 15
3.2 Deskripsi Sistem 18

3.2.1 Skenario Pengujian 18
3.3 Kebutuhan Sistem 19
3.3.1 Perangkat Lunak 19
3.3.2 Perangkat Keras 20
3.3.3 Spesifikasi Perangkat 20
3.4 Instalasi *Virtual Machine* pada VMWare Workstation 21
3.5 Konfigurasi Ubuntu menjadi Router PC 22
3.6 Instalasi Apache2 dan Zabbix 23
3.7 Konfigurasi Snort 25
3.8 Simulasi Snort 26
3.9 Perencanaan Pengukuran 27
3.9.1 Pengukuran Rules Snort 27
3.9.2 Pengukuran Total Paket yang Datang 27
3.9.3 Pengukuran dengan Snort 27
3.9.4 Pengukuran *Network Traffic* 28
BAB IV 29
PENGUJIAN DAN ANALISA SISTEM 29
4.1 Pengujian Snort Tanpa *Rule* dan Dengan *Rule* 29
4.2 Pengukuran Total Paket yang Datang 30
4.3 Pengukuran dengan Snort 35
4.4 Pengukuran *Network Traffic* 39
BAB V 42
PENUTUP 42
5.1 Kesimpulan 42
5.2 Saran 42
DAFTAR PUSTAKA 44
LAMPIRAN A .....
LAMPIRAN B .....