# DAFTAR ISI

ABSTRAK ..... i
ABSTRACK ..... ii
KATA PENGANTAR ..... iii
DAFTAR ISI ..... v
DAFTAR GAMBAR ..... viii
DAFTAR TABEL ..... x
DAFTAR LAMPIRAN ..... xi
BAB 1 PENDAHULUAN ..... 1
1.1 Latar Belakang Masalah ..... 1
1.2 Perumusan Masalah ..... 2
1.3 Maksud dan Tujuan ..... 2
1.4 Batasan Masalah ..... 3
1.5 Metodelogi Penelitian ..... 3
1.5.1 Studi Pustaka ..... 3
1.5.2 Studi Lapangan ..... 3
1.5.3 Metode Pembanguan *Server Monitoring* ..... 4
1.6 Sistematika Penulisan ..... 4
BAB 2 LANDASAN TEORI ..... 7
2.1 Profile Tempat Penelitian ..... 7
2.1.1 Sejarah Instansi ..... 7
2.1.2 Visi dan Misi ..... 9
2.1.3 Logo Diskominfo ..... 10
2.1.4 Struktur Organisasi ..... 12
2.1.5 Deskripsi Pekerjaan ..... 12
2.2 Landasan Teori ..... 30
2.2.1 Pengertian Sistem ..... 30
2.2.2 Pengertian Jaringan Komputer ..... 30
2.2.3 Jenis Jenis Jaringan Komputer ..... 31

2.2.4 ETHERNET .....32
2.2.5 Topologi Jaringan.....33
2.2.6 Pengertian Protokol.....37
2.2.7 Jenis-jenis Protokol.....37
2.2.8 MODEL OSI.....39
2.2.9 TCIP/IP .....44
2.2.10 Perangkat Jaringan Komputer.....45
2.2.11 Pengertian OSSIM .....46
2.2.11.1 Arsitektur OSSIM .....46
2.2.11.2 HIDS(*HOST INTRUSION DETECTION SYSTEM*) .....47
2.2.11.3 Fungsi OSSIM.....48
2.2.12 SIEM .....50
2.2.13 OSSEC .....51
BAB 3 ANALISIS DAN PERANCANGAN .....53
3.1 Analisis Sistem.....53
3.1.1 Analisis Masalah .....54
3.1.2 Analisis Sistem Yang Sedang Berjalan .....54
3.1.3 Solusi yang Diusulkan.....55
3.1.4 Keuntungan Pembangunan *Server* OSSIM.....55
3.2 Analisis Topologi Jaringan Komputer .....55
3.2.1 Analisis Jaringan Diskominfo.....56
3.2.2 Analisis Pengalamatan IP Diskominfo.....58
3.2.3 Analisis *Server* Diskominfo.....58
3.3 Analisis Kebutuhan Komputer Pembangunan *Server*.....59
3.3.1 Kebutuhan Perangkat Keras.....59
3.3.2 Kebutuhan Perangkat Lunak.....59
3.4 Analisis Kebutuhan Komputer *Agent*.....59
3.5 Analisis Pengguna.....59
3.6 Perancangan Sistem .....60
3.6.1 Konfigurasi Sistem.....60
3.6.1.1 Konfigurasi *Host*.....61

3.6.1.2 Konfigurasi Tambah *Agent* .....62
3.6.1.3 Konfigurasi *Policy* .....64
3.6.1.4 Konfigurasi *Directive Rule* .....65
3.6.2 Simulasi Pengujian Sistem.....65
BAB 4 IMPLEMENTASI DAN HASIL PENGUJIAN .....67
4.1 Implementasi OSSIM.....67
4.2 Pengamatan Trafik Jaringan.....68
4.3 Pengujian Terhadap OSSIM .....76
4.3.1 Top 10 *attcker Host*.....76
4.3.2 Top 10 *attacked Host* .....76
4.3.3 *Log* Penyerangan.....81
BAB 5 KESIMPULAN DAN SARAN.....83
5.1 Kesimpulan .....83
5.2 Saran.....83
DAFTAR PUSTAKA .....85