

**SISTEM MONITORING DETEKSI PENYUSUP DALAM JARINGAN
KOMPUTER MENGGUNAKAN SNORT PADA UBUNTU 12.04
BERBASIS SMS GATEWAY**

SKRIPSI



disusun oleh

Etana Diarta

09.11.2587

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2013**

**SISTEM MONITORING DETEKSI PENYUSUP DALAM JARINGAN
KOMPUTER MENGGUNAKAN SNORT PADA UBUNTU 12.04
BERBASIS SMS GATEWAY**

Skripsi

untuk memenuhi sebagai persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Etana Diarta

09.11.2587

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2013**

PERSETUJUAN

SKRIPSI

**SISTEM MONITORING DETEKSI PENYUSUP DALAM JARINGAN
KOMPUTER MENGGUNAKAN SNORT PADA UBUNTU 12.04
BERBASIS SMS GATEWAY**

yang dipersiapkan dan disusun oleh :

Etana Diarta

09.11.2587

telah disetujui oleh dosen pembimbing
pada tanggal 8 Oktober 2012

Dosen Pembimbing



Melwin Syafrizal, S.Kom, M.Eng
NIK. 190302105

PENGESAHAN

SKRIPSI

SISTEM MONITORING DETEKSI PENYUSUP DALAM JARINGAN KOMPUTER MENGGUNAKAN SNORT PADA UBUNTU 12.04 BERBASIS SMS GATEWAY

Etana Diarta

09.11.2587

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 April 2013

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

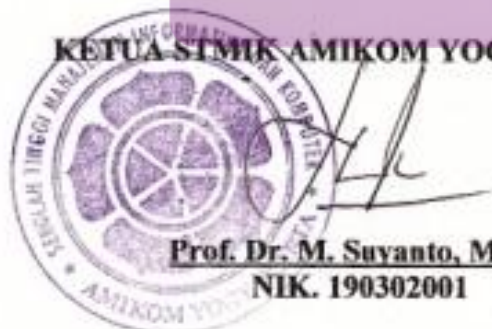
Melwin Syafrizal, S.Kom, M.Eng
NIK. 190302105

Mei P Kurniawan, M.Kom
NIK. 190302187

M. Rudyanto Arief, MT
NIK. 190302098

Skripsi ini telah disahkan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 1 Mei 2013

KETUA STMIK AMIKOM YOGYAKARTA



Prof. Dr. M. Suyanto, M. M.
NIK. 190302001

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 25 April 2013



Etana Diarta
NIM. 09.11.2587

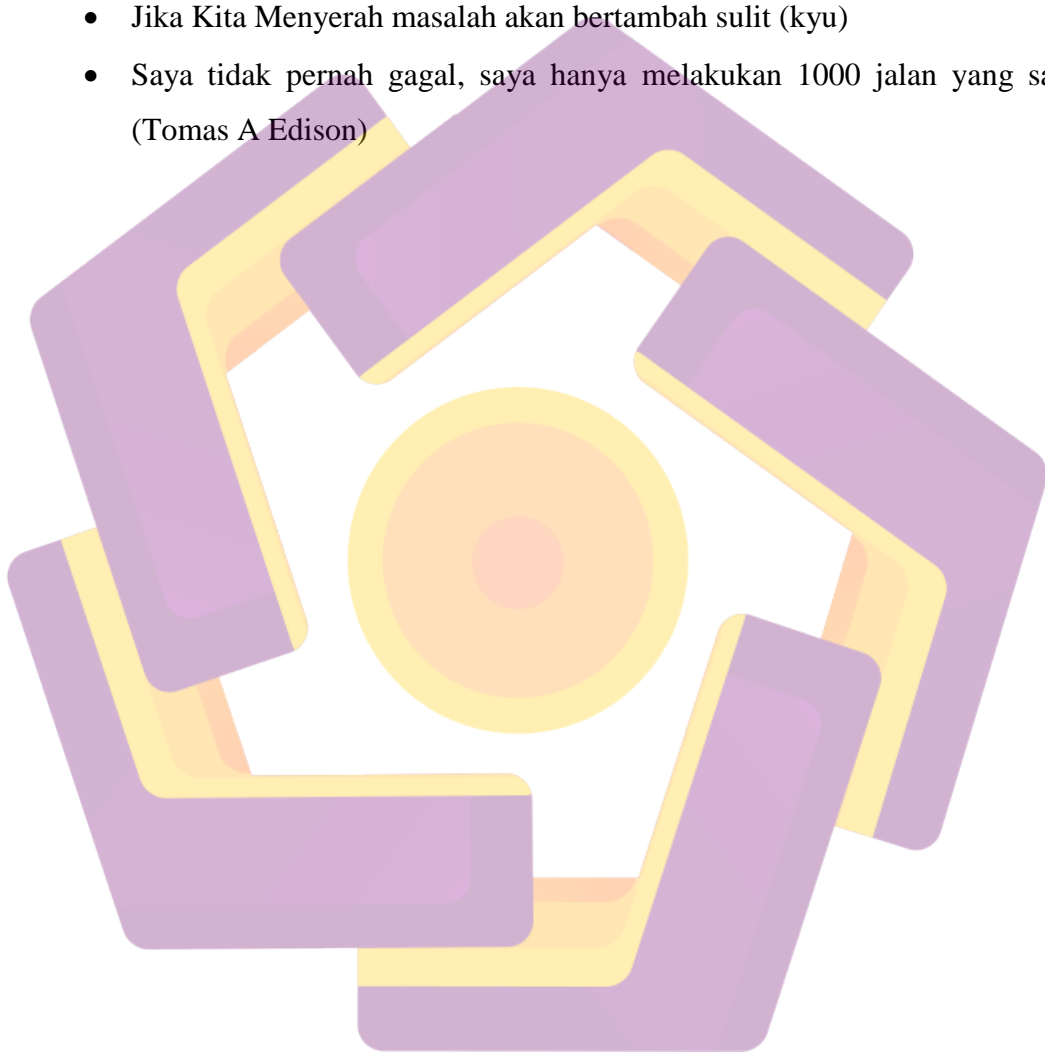
HALAMAN PERSEMBAHAN

Saya ucapkan syukur Alhamdulillah kekhadirat Allah S.W.T. atas semua karunia, hidayah dan inayah-Nya, sehingga akhirnya aku bisa menyelesaikan studiku. Sholawat serta salam aku limpahkan kepada junjungan nabi besar Muhammad S.A.W. yang telah memberikan teladannya kepadaku, semoga aku bisa mengikuti teladanmu. Dan akhirnya saya persembahkan Skripsi ini untuk :

- OrangTuaku yang selalu kasih suport untuk ngerjain skripsinya
- Kakakku yang selalu mendukungku dengan tulus dan tanpa pamrih
- Temen yang selalu aku sandera tekno, pujinato, dan mas agung
- Para sohibku likin, atok, ponco, olis, andri, adit, anggar, ratna, ika, ikanz, silvi, jatu, satya, flo, paksi, ate
- Temen-temen 09TI01 sek paling keren dan paling tuo dewe, kalian is the best
- Anak-anak Onegai Shelter, tetep kompak dan kreatif ya
- Komunitas JNC, mari jlog bersama
- Semua Dosen, karyawan dan penghuni atau civitas akademik STMIK Amikom Yogyakarta. Aku bangga menjadi Mahasiswa di sini. Hidup Amikom!
- Perpust kota Yogyakarta yang telah memberikan segudang inspirasi

HALAMAN MOTTO

- “Hai orang-orang yang beriman, Jadikanlah sabar dan shalatmu Sebagai penolongmu, sesungguhnya Allah beserta orang-orang yang sabar” (Al-Baqarah: 153)
- Jika Kita Menyerah masalah akan bertambah sulit (kyu)
- Saya tidak pernah gagal, saya hanya melakukan 1000 jalan yang salah (Tomas A Edison)



KATA PENGANTAR

Assalamualaikum Wr.Wb.

Segala puji dan syukur, alhamdulillah. Saya persembahkan kehadiran Allah SWT yang telah memberikan rahmat dan karunianya, sehingga penulis dapat menyelesaikan Skripsi ini dengan judul “ **SISTEM MONITORING DETEKSI PENYUSUP DALAM JARINGAN KOMPUTER MENGGUNAKAN SNORT PADA UBUNTU 12.04 BERBASIS SMS GATEWAY**“ yang merupakan salah satu persyaratan untuk menyelesaikan program studi Strata 1 dalam bidang Teknik Informatika di STMIK “AMIKOM” Yogyakarta

Penulis menyadari sepenuhnya bahwa penulisan tugas akhir jauh dari sempurna, penulis mengharapkan kritik dan saran yang bersifat membangun guna membantu tugas akhir ini.

Pada kesempatan ini penulis menyampaikan rasa hormat dan terima kasih kepada:

- 1 Prof. Dr. M. Suyanto, MM. Selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer STMIK“AMIKOM” Yogyakarta.
- 2 Bapak Sudarmawan, M.T. Selaku Kepala Jurusan Teknik Informatika.
- 3 Bapak Melwin Syafrizal, S.Kom, M.Eng. Selaku dosen pembimbing.
- 4 Semua pihak yang telah membantu dalam menyelesaikan tugas ini.

Akhirnya dengan doa kepada Allah, semoga jasa dan amal baiknya mendapat rahmat dan imbalan yang setimpal dari-Nya (Amin).

Wassalamualaikum Wr.Wb.

Yogyakarta, April 2013

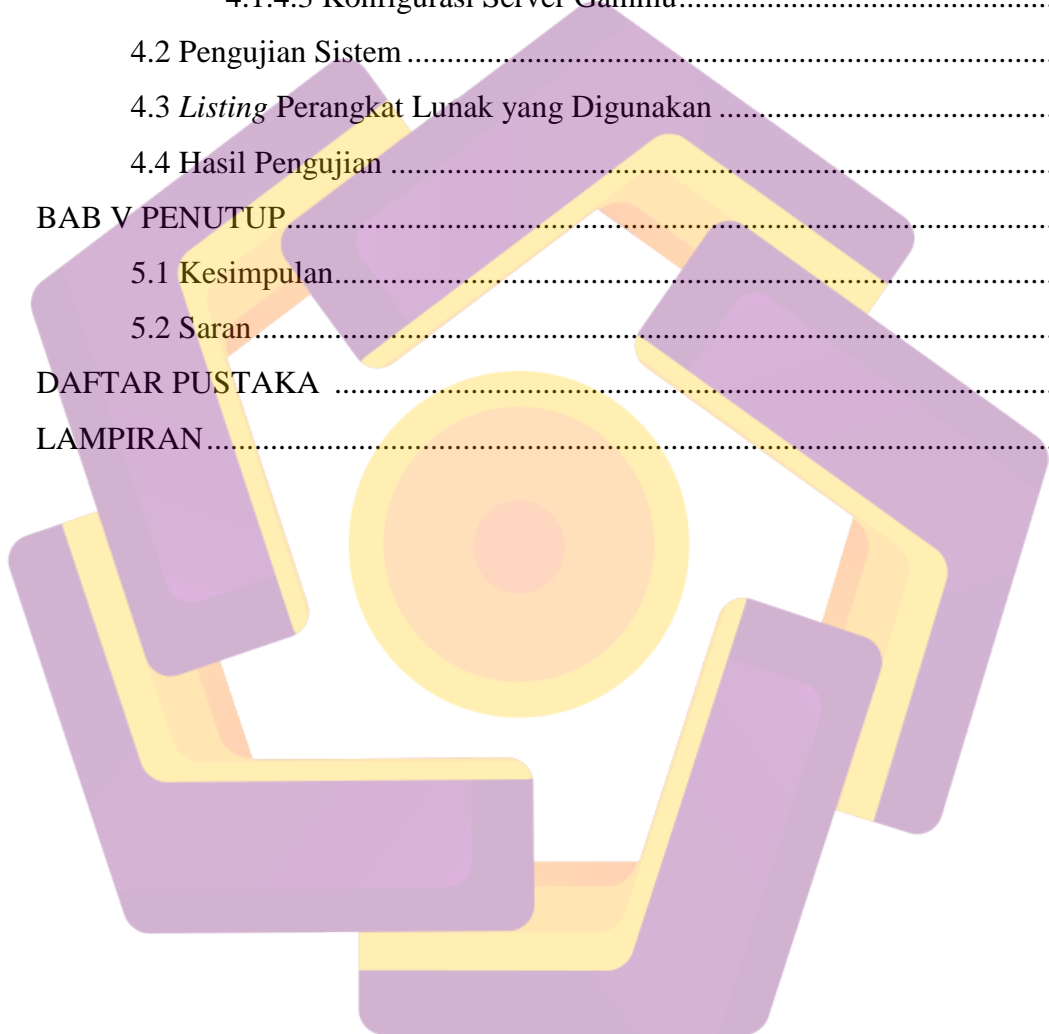
Penulis

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
PERNYATAAN.....	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	vii
KATA PENGATAR.....	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL.....	xiv
INTISARI.....	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metode Penelitian.....	4
1.7 Sistematika Penelitian	4
1.8 Jadwal Kegiatan Penelitian.....	6
BAB II LANDASAN TEORI.....	7
2.1 Tinjauan Pustaka	7
2.2 Pengertian Penyusup (<i>Intruder</i>) Jaringan Komputer	8
2.3 Konsep Dasar Keamanan Jaringan.....	9
2.4 IDS (<i>Intrusion Detection System</i>)	10
2.4.1 Jenis-jenis IDS	11
2.4.2 Cara Kerja IDS	13
2.4.3 Tujuan Penggunaan IDS.....	14

2.5 SMS Gateway.....	15
2.6 Diagram <i>Flowchart</i>	16
2.7 Perangkat Lunak yang Digunakan	16
2.7.1 Snort	17
2.7.2 Gammu	18
2.7.3 MySQL	20
BAB III ANALISIS DAN PERANCANGAN	22
3.1 Analisis Masalah	21
3.1.1 Tindak Penanganan Masalah	25
3.2 Analisis Sistem.....	26
3.2.1 Identifikasi Sistem.....	26
3.2.2 Pemahaman Kerja Sistem.....	26
3.3 Analisis Kebutuhan Sistem	27
3.3.1 Kebutuhan Sistem Fungsional.....	27
3.3.2 Kebutuhan Sistem non Fungsional.....	28
3.4 Perancangan Sistem.....	29
3.4.1 <i>Use Case</i> Diagram.....	29
3.4.2 Perancangan Hubungan Modul-modul Sistem.....	30
3.4.2.1 Penjelasan Komponen Modul.....	31
3.4.3 Flowchart Prosedural IDS	32
3.4.3.1 Penjelasan <i>Flowchart</i>	32
3.4.4 Tabel <i>Database</i>	33
3.4.4.1 Relasi Tabel <i>Database</i>	37
3.5 Rancangan Antar Muka.....	38
BAB IV IMPLEMENTASI DAN PEMBAHASAN SISTEM	40
4.1 Implementasi Sistem	40
4.1.1 Implementasi <i>Webserver</i>	40
4.1.1.1 Instalasi Apache.....	40
4.1.1.2 Instalasi MySql.....	41
4.1.2 Instalasi Snort	42
4.1.2.1 Menentukan Rule Snort yang Digunakan.....	43

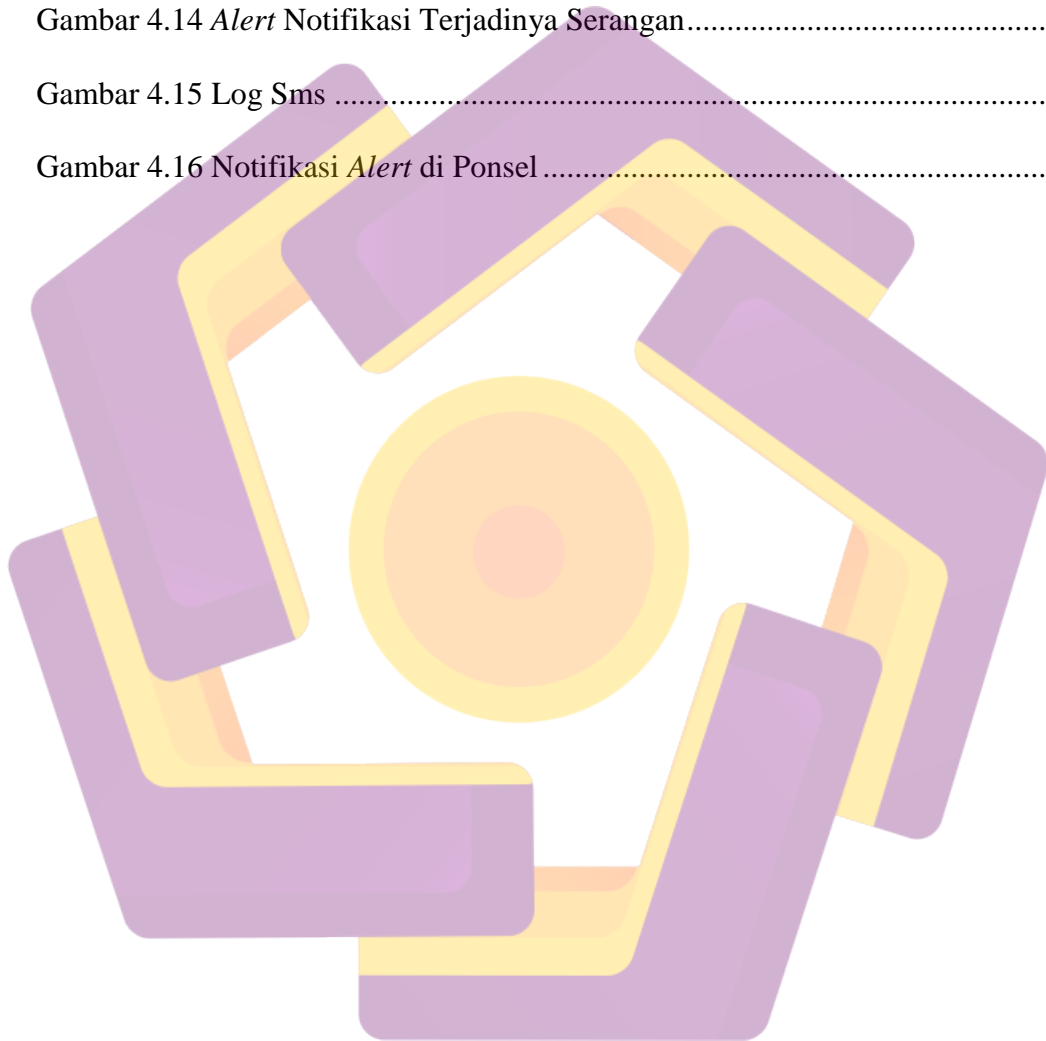
4.1.2.2 Menambahkan <i>Database</i> Snort ke MySql.....	46
4.1.3 Instalasi Acidbase	47
4.1.4 Instalasi Gammu	48
4.1.4.1 Konfigurasi Gammu	49
4.1.4.2 Konfigurasi Koneksi Snort ke Gammu	51
4.1.4.3 Konfigurasi Server Gammu.....	52
4.2 Pengujian Sistem	55
4.3 <i>Listing</i> Perangkat Lunak yang Digunakan	57
4.4 Hasil Pengujian	58
BAB V PENUTUP	59
5.1 Kesimpulan.....	59
5.2 Saran.....	59
DAFTAR PUSTAKA	61
LAMPIRAN	62



DAFTAR GAMBAR

Gambar 2.1 Alur Kegiatan IDS (<i>Intrusion Detection System</i>).....	13
Gambar 2.2 Infrastruktur IDS (<i>Intrusion Detection System</i>)	14
Gambar 2.3 Alur Kerja Gammu.....	19
Gambar 3.1 Grafik Insiden Penyusupan Keamanan Jaringan 2010 – 2012.....	22
Gambar 3.2 Grafik Jenis Penyusupan Keamanan Jaringan 2010 – 2012	23
Gambar 3.3 Alur Kerja Snort berbasis SMS Gateway.....	27
Gambar 3.4 Rancangan Use Case	30
Gambar 3.5 Diagram Hubungan Antar Modul	30
Gambar 3.6 <i>Flowchart</i> Sistem Monitoring Penyusup.....	32
Gambar 3.7 Relasi Tabel <i>Database</i>	37
Gambar 3.8 Tampilan Sistem Monitoring Penyusup Pada Komputer.....	38
Gambar 3.9 Tampilan Sistem Monitoring Penyusup Pada Ponsel	39
Gambar 4.1 Instalasi Apache	40
Gambar 4.2 Apache Berhasil <i>Running</i>	41
Gambar 4.3 Instalasi PHP	41
Gambar 4.4 Tampilan phpMyadmin	42
Gambar 4.5 Instalasi Snort.....	43
Gambar 4.6 Instalasi Berhasil <i>Running</i>	43
Gambar 4.7 Tampilan phpMyadmin setelah ditambah <i>database</i> Snort.....	46
Gambar 4.8 Tampilan Acidbase.....	47
Gambar 4.9 Instalasi Gammu.....	48

Gambar 4.10 Gammu Berhasil <i>Running</i>	48
Gambar 4.11 Tes Identitas device	50
Gambar 4.12 Server Gammu	55
Gambar 4.13 <i>Scanning</i> dengan Angry IP	55
Gambar 4.14 <i>Alert</i> Notifikasi Terjadinya Serangan.....	56
Gambar 4.15 Log Sms	56
Gambar 4.16 Notifikasi <i>Alert</i> di Ponsel	57



DAFTAR TABEL

Tabel 2.1 Simbol-simbol <i>Flowchart</i>	17
Tabel 3.1 Simbol Simbol Pada <i>Use Case</i>	29
Tabel 3.2 Tabel iphdr	33
Tabel 3.3 Tabel opt	33
Tabel 3.4 Tabel tcphdr	34
Tabel 3.5 Tabel detail.....	34
Tabel 3.6 Tabel icmphdr	34
Tabel 3.7 Tabel data.....	34
Tabel 3.8 Tabel encoding.....	35
Tabel 3.9 Tabel event.....	35
Tabel 3.10 Tabel reference.....	35
Tabel 3.11 Tabel reference_system.....	35
Tabel 3.12 Tabel sig_reference	35
Tabel 3.13 Tabel schema.....	35
Tabel 3.14 Tabel sensor	36
Tabel 3.15 Tabel signature	36
Tabel 3.16 Tabel sig_class	36
Tabel 3.17 Tabel udphdr	36
Tabel 4.1 Listing Rule.....	44
Tabel 4.2 Listing Perangkat Lunak	57

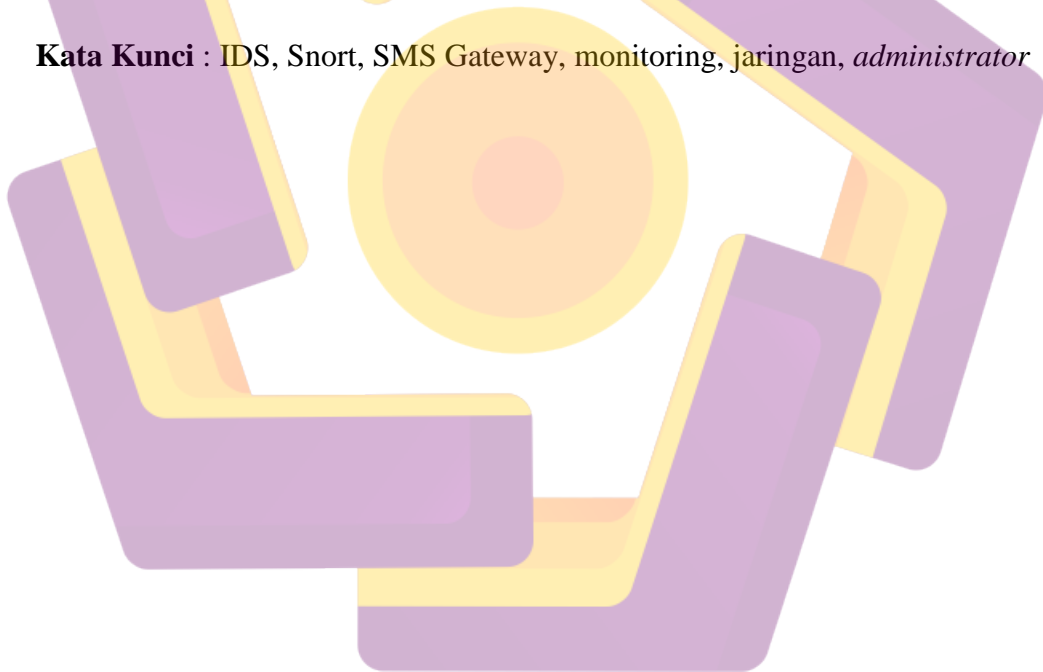
INTISARI

Perkembangan teknologi informasi dewasa ini semakin cepat, hal ini membuat keamanan jaringan menjadikan hal yang penting. Semakin banyaknya komputer yang terhubung menghasilkan banyak celah-celah pada suatu jaringan. Seorang *administrator* mempunyai peran penting dalam melindungi keamanan jaringan. Masalah datang ketika seorang *administrator* mengalami masalah manusiawi seperti sakit, lalai, capek sedangkan diwaktu yang sama membutuhkan informasi yang cepat ketika terjadi penyusupan jaringan.

Permasalahan tersebut dapat diatasi dengan menambahkan sistem pendeteksi lalu lintas data yang dikenal sebagai *Intrusion Detection System (IDS)*. IDS ini nantinya akan dihubungkan dengan SMS *gateway* sehingga *administrator* dapat menerima notifikasi berupa *alert* ketika terjadi penyusupan terhadap jaringan kapanpun dan dimanapun.

Pada skripsi ini, penulis mencoba untuk melakukan analisis dan pengujian pada pokok – pokok bahasan di atas sehingga menghasilkan sistem yang mampu mendeteksi adanya penyusup pada suatu jaringan yang bersifat *mobile*.

Kata Kunci : IDS, Snort, SMS Gateway, monitoring, jaringan, *administrator*



ABSTRACT

Development of information technology nowadays more faster, this makes network security become important. Increasing number of computers that are connected making a lot of gaps in a network. An administrator has an important role in protecting the security of the network. The problem comes when an administrator having human problems such as pain, negligence, tired while at the same time need the rapid information when there is an intrusion on the network.

This problem can be solved by adding data traffic detection system known as Intrusion Detection System (IDS). IDS will be connected to SMS gateway until that administrators can receive notifications such as alerts during an intrusion to the network anytime and anywhere.

In this thesis, the author tries to do analysis and testing on the subjects above so as to produce a system capable of detecting the intruder in a network that are mobile.

Keyword : IDS, Snort, SMS Gateway, monitoring, network, administrators

