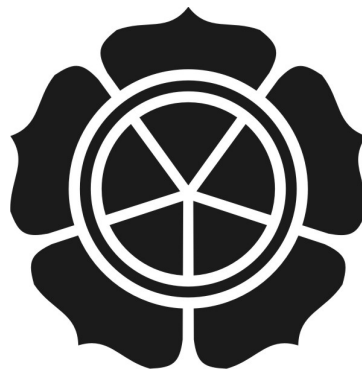


**AUTO CAPTURE FILE LOG PADA INTRUSION PREVENTION
SYSTEM (IPS) SAAT TERJADI SERANGAN PADA
JARINGAN KOMPUTER**

SKRIPSI



disusun oleh

Ashari Abriando

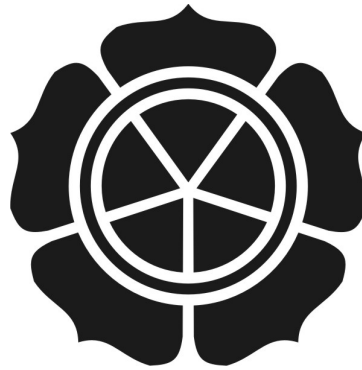
10.11.4179

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

**AUTO CAPTURE FILE LOG PADA INTRUSION PREVENTION
SYSTEM (IPS) SAAT TERJADI SERANGAN PADA
JARINGAN KOMPUTER**

SKRIPSI

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



disusun oleh

Ashari Abriando

10.11.4179

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

PERSETUJUAN

SKRIPSI

**AUTO CAPTURE FILE LOG PADA INTRUSION PREVENTION
SYSTEM (IPS) SAAT TERJADI SERANGAN PADA
JARINGAN KOMPUTER**

yang dipersiapkan dan disusun oleh

Ashari Abriando

10.11.4179

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Oktober 2013

Dosen Pembimbing,



Melwin Syafrizal, S.Kom, M.Eng

NIK. 190302105

PENGESAHAN

SKRIPSI

**AUTO CAPTURE FILE LOG PADA INTRUSION PREVENTION
SYSTEM (IPS) SAAT TERJADI SERANGAN PADA
JARINGAN KOMPUTER**

yang dipersiapkan dan disusun oleh

Ashari Abriando

10.11.4179

telah dipertahankan di depan Dewan Penguji
pada tanggal 06 Maret 2014

Susunan Dewan Penguji

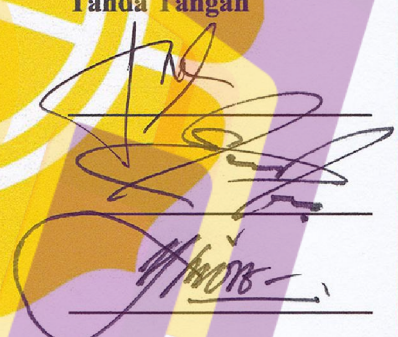
Nama Penguji

Tanda Tangan

Joko Dwi Santoso, M.Kom.
NIK. 190302181

Tonny Hidayat, M.Kom.
NIK. 190302182

Heri Sismoro, M.Kom.
NIK. 190302057



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
tanggal 07 Maret 2014

KETUA STMIK AMIKOM YOGYAKARTA



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

PERNYATAAN KEASLIAN

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

Yogyakarta, 07 Maret 2014

Ashari Abriando
NIM. 10.11.4179

MOTTO

"Sesungguhnya sesudah kesulitan itu ada kemudahan. Maka apabila kamu Telah selesai (dari sesuatu urusan), kerjakanlah dengan sungguh-sungguh (urusan) yang lain. Dan Hanya kepada Tuhanmulah hendaknya kamu berharap."

(Qs. Al-Insyirah 94 : 6-8)

"Barang siapa berjalan untuk menuntut ilmu maka Allah akan memudahkan baginya jalan ke surga." (HR. Muslim)

Tidak ada masalah yang tidak bisa diselesaikan selama ada komitmen bersama untuk menyelesaikannya

Jenius adalah 1 % inspirasi dan 99 % keringat. Tidak ada yang dapat menggantikan kerja keras

PERSEMBAHAN

Puji syukur penulis panjatkan kehadirat Allah SWT, atas rahmat, limpahan karunia, serta hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi ini. Sholawat dan salam penulis haturkan kepada Nabi Muhammad SAW yang telah membawa dunia ini hijrah dari zaman yang jahiliah, ke zaman yang penuh dengan ilmu. Pada kesempatan ini, penulis juga tidak lupa mengucapkan terimakasih kepada :

1. Kedua orang tua, mama dan papa serta adik tercinta, Shintia Ayu Rianelsa yang telah memberikan banyak dukungan baik moril maupun materil dan do'a, kasih sayang, perhatiannya untuk putra-mu ini ☺.
2. Bapak Melwin Syafrizal, S.Kom, M.Eng selaku dosen pembimbing atas segala bimbingan dan masukannya guna penyempurnaan skripsi ini.
3. Teman-teman seperjuangan dari kelas 10-S1TI-08, yang banyak memberikan dukungan dalam penyusunan skripsi ini. Restu Anggoro, Meylinda, Siska, Ati'atul, Dipa, Unik, Ayyas, Mega, Afif, Yayan, Didit, Anwar, Rendi, Sandi, dkk. Terima kasih atas dukungan dan semangat kalian. ☺
4. Teman-teman partner bidang IT. Rian Adi Wibowo, Ageng Juniar, Bambang Sumarsono, Punditya Derry, Rahman Kurnia, dkk yang telah banyak berkontribusi dalam penyusunan skripsi ini.
5. Sahabat-sahabat sehidup sehutangan kost sukun 26, M. Noko Darpito, Bayu Putra, Edi Wantono, Nanto Badhra, Teguh Ardiyansah, Tri Nugraha, terimakasih atas dukungan, semangat, canda tawa, ejekan, celaan, dan nasehat kalian selama ini ☺.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Dengan mengucapkan syukur kepada Allah SWT yang telah memberi rahmat dan hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan skripsi ini dengan judul “Auto Capture File Log pada Intrusion Prevention System (IPS) Saat Terjadi Serangan pada Jaringan Komputer”, yang merupakan salah satu persyaratan untuk menyelesaikan program studi Strata 1 dalam bidang Teknik Informatika di STMIK AMIKOM Yogyakarta.

Penulis menyadari sepenuhnya bahwa penulisan skripsi ini jauh dari sempurna, penulis mengharapkan kritik dan saran yang bersifat membangun guna membantu skripsi ini menjadi lebih baik.

Pada kesempatan ini penulis menyampaikan rasa hormat dan terimakasih kepada :

1. Prof. Dr. M. Suyanto, MM. Selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Melwin Syafrizal, S.Kom, M.Eng. Selaku dosen pembimbing.
3. Semua pihak yang telah membantu dalam menyelesaikan skripsi ini.

Akhirnya dengan do'a kepada Allah *Subhanahu Wa Ta'ala* semoga laporan skripsi ini bermanfaat bagi semua pihak.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 07 Maret 2014

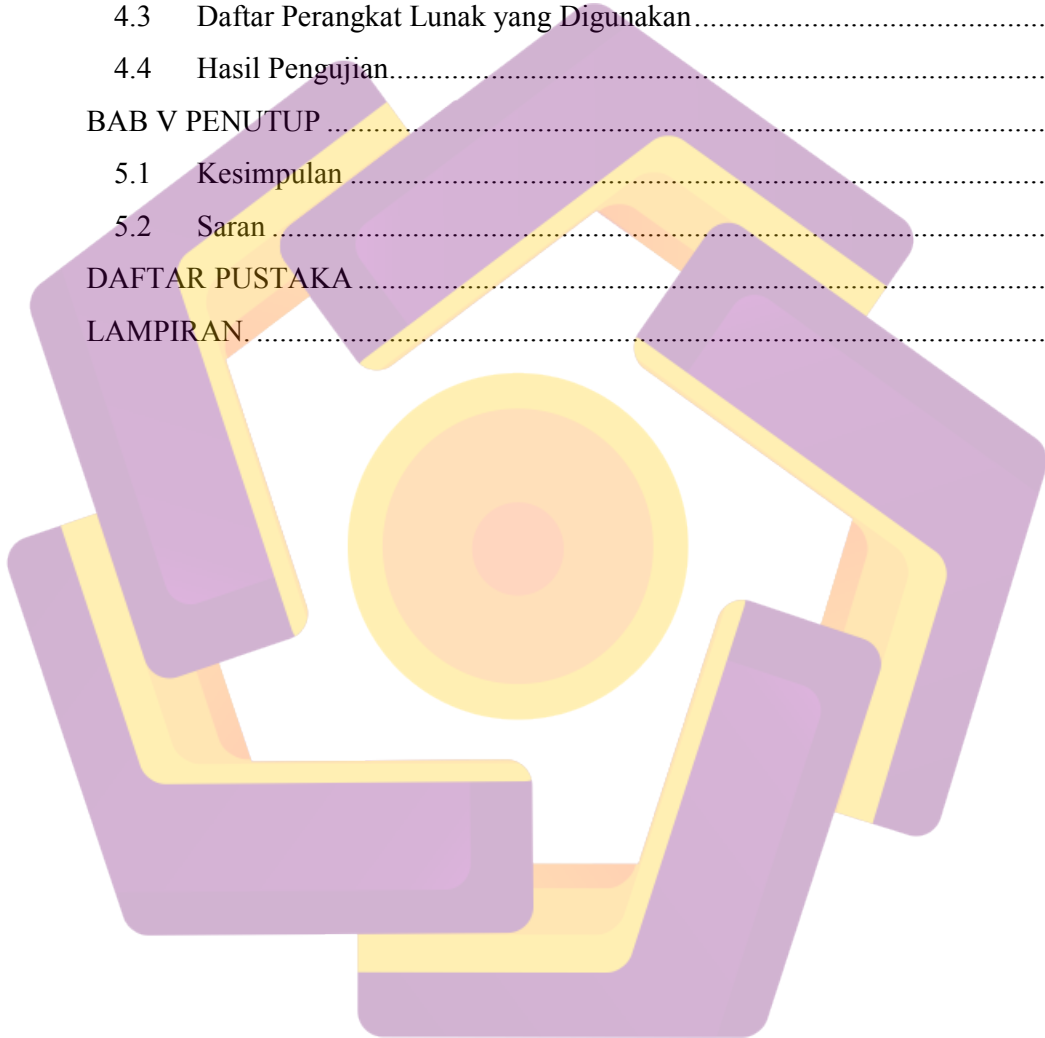
Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN	iv
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
INTISARI	xiv
ABSTRACT	xv
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	5
1.8 Rencana Kegiatan Penelitian	6
BAB II LANDASAN TEORI	7
2.1 Tinjauan Pustaka	7
2.2 Konsep Dasar Jaringan Komputer	8
2.3 Konsep Dasar Keamanan Jaringan	9
2.4 Pengertian Penyusup (<i>Intruder</i>) Jaringan Komputer	11
2.5 <i>Intrusion Prevention System (IPS)</i>	11

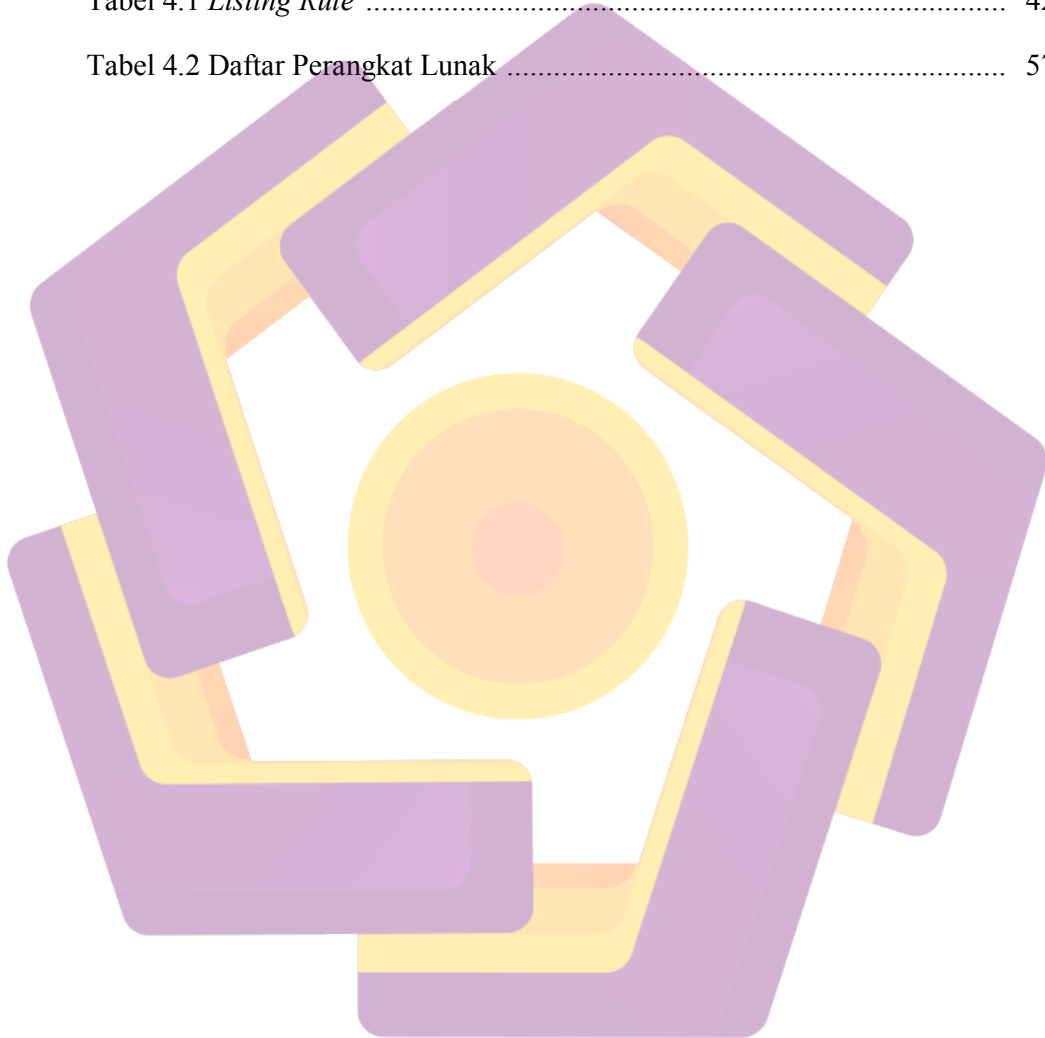
2.5.1	Jenis-jenis IPS	12
2.5.2	Cara Kerja IPS.....	14
2.5.3	NIPS (<i>Network-based Intrusion Prevention System</i>)	15
2.5.4	Implementasi IPS dalam Mengamankan Jaringan Komputer.....	16
2.5.5	Topologi IPS	17
2.6	<i>Intrusion Detection System</i> (IDS).....	17
2.6.1	Cara Kerja IDS	18
2.6.2	Tujuan penggunaan IDS (<i>Intrusion Detection System</i>).....	19
2.7	Diagram <i>Flowchart</i>	20
2.8	Perangkat Lunak (<i>Software</i>) yang Digunakan	22
2.8.1	Snort.....	22
2.8.2	Iptables.....	23
2.8.3	MySQL	24
BAB III ANALISIS DAN PERANCANGAN SISTEM		26
3.1	Analisis Masalah	26
3.2	Analisis Kelemahan Sistem.....	29
3.2.1	Topologi dalam Perancangan IPS	29
3.2.2	Kelemahan Sistem Keamanan Jaringan yang Digunakan	29
3.2.3	Tindak Penanganan Masalah.....	30
3.3	Analisis Sistem.....	31
3.3.1	Identifikasi Sistem.....	31
3.3.2	Pemahaman Kerja Sistem	31
3.4	Analisis Kebutuhan Sistem	32
3.4.1	Kebutuhan Sistem Fungsional.....	32
3.4.2	Kebutuhan Sistem Non Fungsional	32
3.4.2.1	Kebutuhan Perangkat Keras (<i>Hardware</i>).....	33
3.4.2.2	Kebutuhan Perangkat Lunak (<i>Software</i>)	33
3.5	Perancangan Sistem.....	33
3.5.1	Perancangan Hubungan Modul-Modul Sistem	34
3.5.2	Flowchart Prosedural IPS	35
3.6	Rancangan Antar Muka (<i>Interface</i>).....	36

BAB IV IMPLEMENTASI DAN PEMBAHASAN	38
4.1 Implementasi Sistem.....	38
4.1.1 Implementasi Webserver	38
4.1.1.1 Instalasi Apache2.....	38
4.2 Pengujian Sistem	56
4.2.2.1 Tampilan File Log	56
4.3 Daftar Perangkat Lunak yang Digunakan.....	57
4.4 Hasil Pengujian.....	58
BAB V PENUTUP	59
5.1 Kesimpulan	59
5.2 Saran	60
DAFTAR PUSTAKA	61
LAMPIRAN.....	1



DAFTAR TABEL

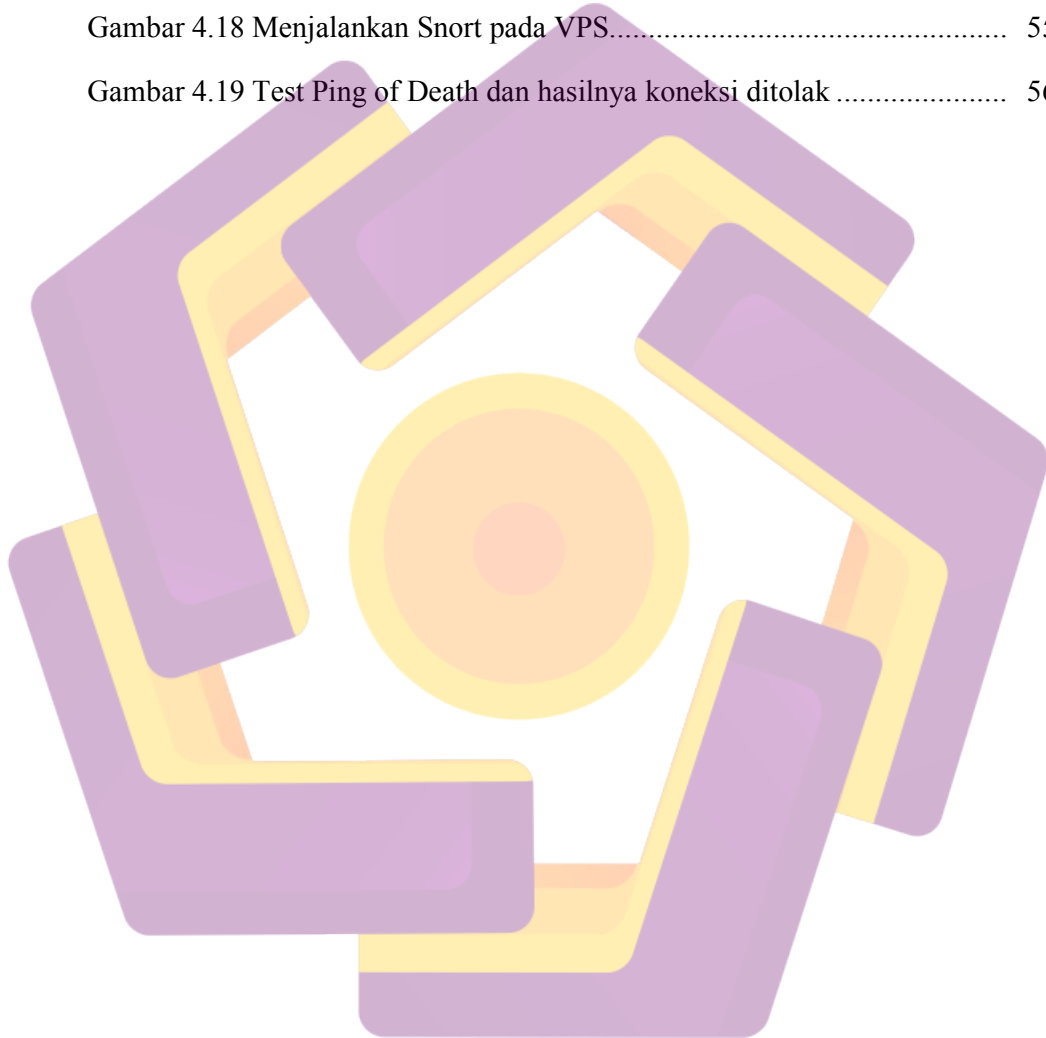
Tabel 1.1 Rencana Penelitian	6
Tabel 2.1 Simbol-simbol <i>Flowchart</i>	21
Tabel 4.1 <i>Listing Rule</i>	42
Tabel 4.2 Daftar Perangkat Lunak	57



DAFTAR GAMBAR

Gambar 2.1 <i>Network-based Intrusion Prevention System (NIPS)</i>	16
Gambar 2.2 Topologi dan terminologi dalam implementasi IPS	17
Gambar 2.3 Alur Kegiatan IDS (<i>Intrusion Detection System</i>)	18
Gambar 2.4 Infrastruktur IDS (<i>Intrusion Detection System</i>)	19
Gambar 3.1 Grafik insiden penyusupan keamanan jaringan 2012 – 2013	26
Gambar 3.2 Grafik jenis penyusupan keamanan jaringan 2012 – 2013	27
Gambar 3.3 Rancangan topologi yang digunakan	29
Gambar 3.4 Diagram Hubungan Antar Modul	34
Gambar 3.5 Flowchart Auto Capture File Log pada IPS	35
Gambar 3.6 Tampilan auto capture file log pada Intrusion Prevention System	36
Gambar 4.1 Proses Update Packet	38
Gambar 4.2 Instalasi Apache2 dan php5	39
Gambar 4.3 Menjalankan Apache2	39
Gambar 4.4 Instalasi MySQL Server	39
Gambar 4.5 Tampilan PHPMyAdmin	40
Gambar 4.6 Proses Instalasi Snort	41
Gambar 4.7 Menjalankan Snort	42
Gambar 4.8 Edit file <code>/etc/snort/rules/local.rules</code>	45
Gambar 4.9 Tampilan database snort pada phpmyadmin	47
Gambar 4.10 Tampilan AcidBASE	48
Gambar 4.11 Konfigurasi iptables	49
Gambar 4.12 Test Ping of Death sebelum menjalankan tool Snort	50

Gambar 4.13 Menjalankan tool iptables	51
Gambar 4.14 Menjalankan tool Snort Gambar 4.14 Menjalankan tool Snort .	52
Gambar 4.15 Test Ping of Death dan hasilnya koneksi ditolak	53
Gambar 4.16 Remote VPS menggunakan Putty	54
Gambar 4.17 Edit file rc.local	54
Gambar 4.18 Menjalankan Snort pada VPS.....	55
Gambar 4.19 Test Ping of Death dan hasilnya koneksi ditolak	56



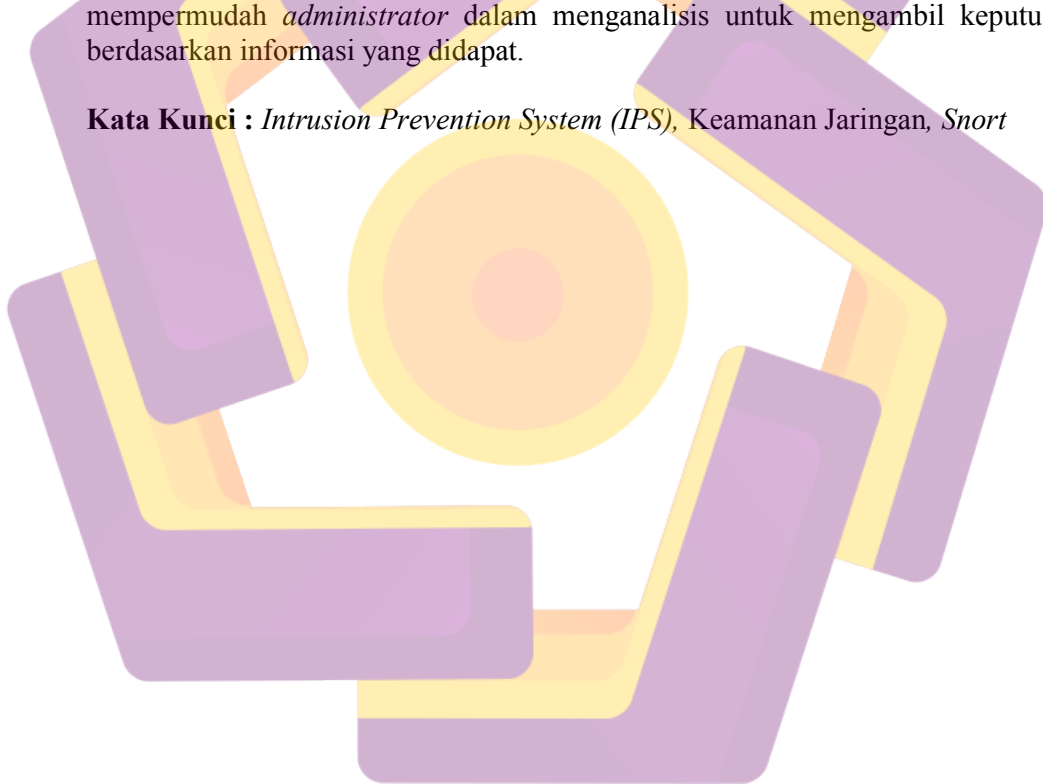
INTISARI

Keamanan pada suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar yang berupa serangan *hacker* ataupun *cracker* yang tujuannya merusak jaringan komputer yang terkoneksi pada internet ataupun mencuri informasi penting pada jaringan tersebut.

Banyak *tool* yang digunakan untuk mengamankan jaringan komputer, misalnya *firewall*, namun *firewall* tidak menjamin sepenuhnya keamanan tersebut. Oleh sebab itu, berkembanglah teknologi *IPS (Intrusion Prevention System)* yang berguna untuk mencegah adanya serangan dari penyusup dan *Snort* yang berguna untuk mengamati aktivitas dalam suatu jaringan komputer.

IPS dan *Snort* sangat membantu dalam mencegah serangan-serangan yang dilakukan oleh *hacker* atau *cracker* tersebut. Dengan tambahan *auto capture* file log, maka setiap serangan yang terjadi dapat didokumentasikan, sehingga mempermudah *administrator* dalam menganalisis untuk mengambil keputusan berdasarkan informasi yang didapat.

Kata Kunci : *Intrusion Prevention System (IPS)*, Keamanan Jaringan, *Snort*



ABSTRACT

Security on a network is often interrupted by the threat from inside or from outside in the form of attacks by hackers or crackers who aim damaged computer networks connected to the Internet or steal important information on the network.

Many tools are used to secure computer networks, such as a firewall, but the firewall does not guarantee the security. Therefore, grew a technology IPS (Intrusion Prevention System) which is useful to prevent any attacks from intruder and Snort are useful for observing activity in a computer network.

IPS and Snort are very helpful in preventing attacks by hackers or crackers. The presence of IPS and Snort these attacks can be prevented or eliminated. With additional auto capture log file, then any attacks can be documented, making it easier for administrators to analyze decisions based on the information obtained.

Keywords : *Intrusion Prevention System (IPS), Network Security, Snort*

