

**ANALISIS DAN PERANCANGAN SISTEM KEAMANAN JARINGAN
MENGUNAKAN NIPS (NETWORK-BASED INTRUSION
PREVENTION SYSTEM) DENGAN METODE
SIGNATURE BASED SYSTEM**

SKRIPSI



Disusun oleh

Habib Abdulloh

13.11.6956

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2020

**ANALISIS DAN PERANCANGAN SISTEM KEAMANAN JARINGAN
MENGUNAKAN NIPS (NETWORK-BASED INTRUSION
PREVENTION SYSTEM) DENGAN METODE
SIGNATURE BASED SYSTEM**

Untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana Komputer
pada Program Studi Informatika



Disusun oleh

Habib Abdullah

13.11.6956

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020**

PERSETUJUAN

SKRIPSI

**ANALISIS DAN PERANCANGAN SISTEM KEAMANAN JARINGAN
MENGUNAKAN NIPS (NETWORK-BASED INTRUSION
PREVENTION SYSTEM) DENGAN METODE
SIGNATURE BASED SYSTEM**

yang dipersiapkan dan disusun oleh

Habib ABdulloh

13.11.6956

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal Agustus 2020

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom

NIK. 190302181

PENGESAHAN

SKRIPSI

**ANALISIS DAN PERANCANGAN SISTEM KEAMANAN JARINGAN
MENGUNAKAN NIPS (NETWORK-BASED INTRUSION
PREVENTION SYSTEM) DENGAN METODE
SIGNATURE BASED SYSTEM**

yang dipersiapkan dan disusun oleh

Habib Abdullah

13.11.6956

telah dipertahankan di depan Dewan Penguji

pada tanggal 20 Juli 2020

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

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

Ichsan Wiratama, S.T., M.Cs
NIK. 190302199

Joko Dwi Santoso, M.Kom
NIK. 190302181

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana Komputer

Tanggal Agustus 2020

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si., M.T.

NIK. 190302038

PERNYATAAN

Saya yang bertandatangan 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 tinggi manapun, 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.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 17 Agustus 2020



Hubib Abdulloh

NIM. 13.11.6956

MOTTO

“Hidup sekali, Hiduplah yang berarti.”

“Menjadi orang penting itu baik, namun lebih penting menjadi orang baik.”

“God will give you better thing than you think the best.”

“Don’t stress do your best forget the rest.” (Devi Khalim A., S.Kom)

“Believe all that happens to you is for good. Even when Allah allows bad things to happen, there’s something good behind it.” (Dr. Bilal Philips)

“Kegagalan bukanlah untuk ditangisi dan disesali. Namun kegagalan untuk ditimba pelajarannya agar tidak terulang lagi.”(Ustd. Dr. Muhammad Arifin Badri)

“Banyak kegagalan dalam hidup ini dikarenakan orang-orang tidak menyadari betapa dekatnya mereka dengan keberhasilan saat mereka menyerah.

“Learn from the past, live for the today, and plan for tomorrow”

PERSEMBAHAN

Segala puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan ahmat, hidayah, kesehatan, kesempatan, pengetahuan, dan kekuatannya, sehingga penulis dapat membuat dan menyelesaikan skripsi ini dengan lancar tanpa halangan yang berarti. Shalawat dan salam juga tercurahkan kepada nabi agung Muhammad SAW yang telah membawa zaman kedamaian dan beradab ke muka bumi.

Dalam kesempatan ini, penulis ingin mengutarakan rasa terimakasih kepada seluruh pihak yang terlibat secara langsung maupun tidak langsung, serta membantu penulis dalam proses menempuh pendidikan, serta menyelesaikan skripsi :

1. Yang pertama Terimakasih yang sebesar-besarnya kepada ke-dua orang tua tercinta Bapak Purwadi Nur Hidayat dan Ibu Mudrikah, adik saya Munawar Hasby yang tidak henti-hentinya selalu mendo'akan, mensupport serta memberi nasihat untuk keberhasilan penulis, serta seluruh anggota keluarga dan kerabat yang tak pernah lelah memberikan dukungan demi kelancaran penulis menyelesaikan pendidikan. Terimakasih.
2. Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing yang dengan sabar membimbing, memberikan banyak nasihat, saran sehingga penulis dapat menyelesaikan skripsi dengan sangat baik.
3. Bapak Melwin Syafrizal, S.Kom., M.Eng. dan juga Bapak Ichsan Wiratama, S.T.,M.Cs., selaku dosen penguji, Terimakasih banyak atas setiap kritik dan saran yang telah diberikan kepada penulis agar bisa menjadi lebih baik lagi.
4. Devi Khalim Aulia yang begitu setia dan sabar mencurahkan segala bentuk perhatian dan dukungannya kepada penulis selama proses pengerjaan skripsi, Terimakasih.
5. Teman-teman seperjuangan di Keluarga Besar HMIF Amikom Yogyakarta : Ibenk, Mustiqa, Nuryadi, Udin, Tri, Sidiq, Devi, bu Ria,

Idham, Amel, Upik, Ootong, Seno, Heri, Ildan, Renaldi, serta teman-teman lain yang tidak bisa disebutkan satu persatu.

6. Keluarga Besar 13-S1TI-03, Bambang, Topek, Sideq, Juni aston, Ami, Lugina, Idham, Deki, Puji, dan semua kawan-kawan satu kelas yang tidak bisa disebutkan satu persatu.
7. Seluruh Dosen STMIK Amikom yang telah memberikan ilmu yang sangat bermanfaat bagi penulis.



KATA PENGANTAR

Asssalamu'alaikum Warahmatullahi Wabarakatuh

Alhamdulillah, puji syukur kehadiran Allah SWT yang telah melimpahkan rahmat, taufik, hidayah, serta inayah-Nya, sehingga penulis dapat menyelesaikan laporan skripsi ini yang berjudul “Analisis dan Perancangan *Sistem Keamanan Jaringan Menggunakan NIPS (Network-Based Intrusion Prevention System) dengan Metode Signature-Based System*”.

Penyusunan laporan ini dimaksudkan sebagai salah satu syarat untuk memperoleh gelar Sarjana S1 pada Program Studi Informatika Fakultas Ilmu Komputer di Universitas Amikom Yogyakarta.

Proses penyusunan hingga selesainya laporan skripsi ini tidak terlepas dari bantuan, bimbingan, dan dukungan dari berbagai pihak baik secara langsung maupun tidak langsung telah memberikan motivasi kepada penulis. Maka dari itu, sebagai rasa hormat penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. H. M. Suyanto, MM selaku Rektor Amikom Yogyakarta.
2. Ibu Krisnawati, S.Si, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Bapak Sudarmawan S.T., M.T. selaku Ketua Jurusan S1 Informatika Universitas Amikom Yogyakarta.
4. Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing yang telah memberikan masukan, arahan, dan motivasi kepada penulis.

5. Segenap staff dan dosen STMIK Amikom Yogyakarta yang telah memberikan ilmunya selama kuliah.
6. Kedua Orang Tua, adik dan segenap keluarga yang telah memberikan dukungan moril serta materil dengan tulus, ikhlas dan penuh kasih sayang.
7. Teman-teman seperjuangan kelas 13-S1TI-03 dan juga teman-teman HMJTI.

Penulis menyadari masih ada kekurangan dari penyusunan laporan skripsi ini. Kritik dan saran yang membangun selalu penulis harapkan demi kemajuan dan arah lebih baik di masa yang akan datang sehingga dapat bermanfaat bagi penulis serta pihak-pihak yang membutuhkan untuk pengembangan serta penelitian selanjutnya. Semoga laporan skripsi ini bermanfaat bagi semua pihak.

Wassalamu'alaikum Warahmatullah Wabarakatuh.

Yogyakarta, 17 Agustus 2020

Habib Abdulloh

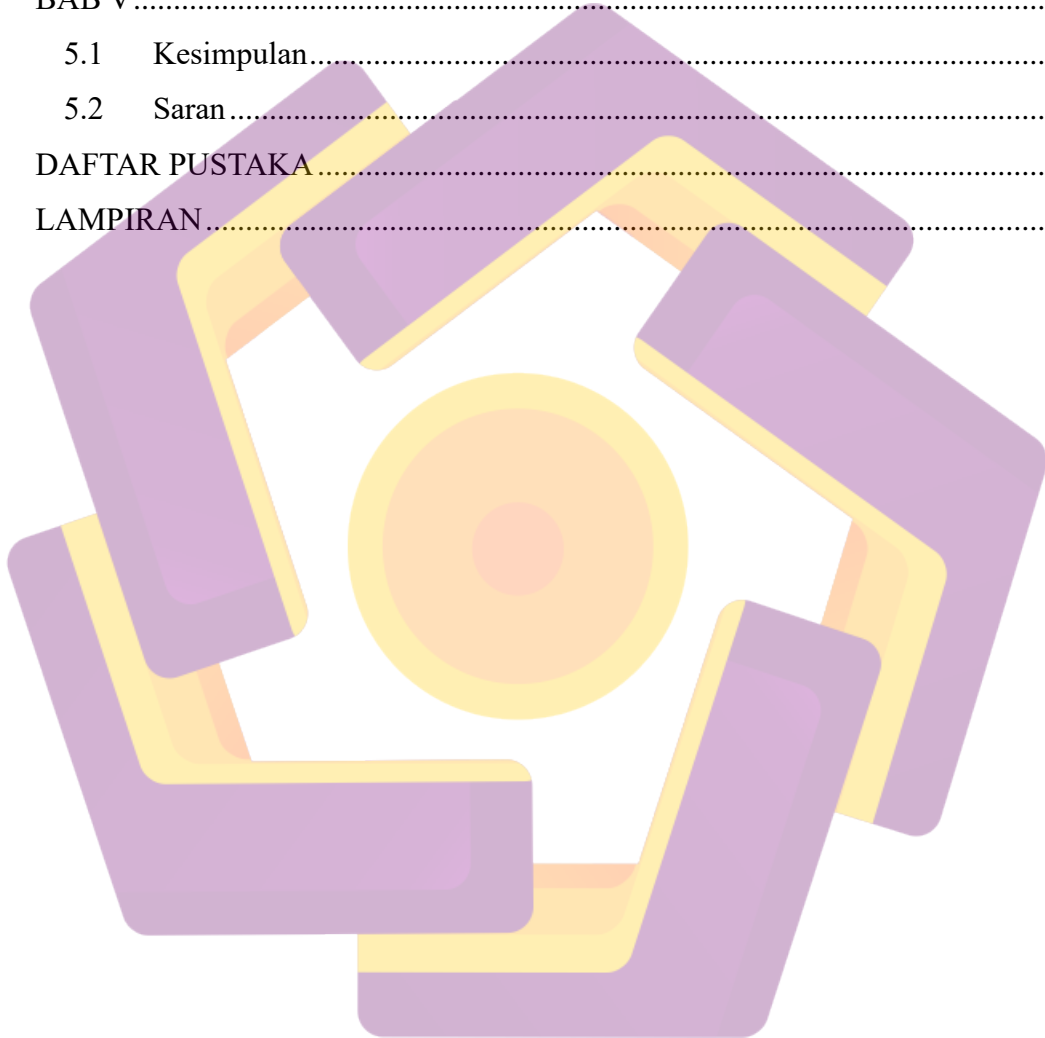
13.11.6956

DAFTAR ISI

COVER	i
PERSETUJUAN	iii
PENGESAHAN	iv
PERNYATAAN	v
MOTTO.....	vi
PERSEMBAHAN.....	vii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR	xv
INTISARI.....	xviii
ABSTRACT.....	xix
BAB I.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Maksud dan Tujuan Penelitian	3
1.4.1 Maksud Penelitian.....	4
1.4.2 Tujuan Penelitian	4
1.4.3 Manfaat Penelitian	4
1.5 Metode Penelitian.....	4
1.5.1 Metode Pengumpulan Data.....	4
1.6 Sistematika Penulisan.....	5
BAB II.....	7
2.1 Tinjauan Pustaka.....	7
2.2 Pengenalan Jaringan Komputer.....	8
2.2.1 Definisi Jaringan	8
2.3 Keamanan Jaringan	9
2.3.1 Prinsip Keamanan Jaringan	9

2.3.2	Jenis-Jenis Serangan Terhadap Keamanan Jaringan.....	9
2.5	Jenis-jenis <i>Intrusion Detection System</i> (IDS).....	12
2.5.1	<i>Host Intrusion Detection System</i> (HIDS).....	12
2.5.2	<i>Network Intrusion Detection System</i> (NIDS).....	12
2.6	<i>Intrusion Prevention System</i> (IPS)	12
2.5.1	Jenis-jenis <i>Intrusion Prevention System</i> (IPS).....	13
2.5.1.1	<i>Host Intrusion Prevention System</i> (HIPS).....	13
2.5.1.2	<i>Network Intrusion Prevention System</i> (NIPS).....	14
2.6	SNORT	15
2.6.1	Komponen-komponen snort	16
2.6.2	Mode-mode pada <i>Snort</i>	17
2.6.5	Kelebihan Snort	20
2.7	Diagram Flowchart.....	21
BAB III	23
3.1	Analisis Masalah	23
3.2	Rencana Tindakan Penanganan Masalah	24
3.2.1	IPS yang Digunakan	25
3.3	Analisa Kebutuhan Sistem	26
3.3.1	Kebutuhan Sistem Fungsional	26
3.3.2	Kebutuhan Sistem Non Fungsional	27
3.4	Perancangan Sistem IPS	29
3.4.1	Desain Topologi IPS	30
3.4.2	Perancangan Hubungan Antar Modul Sistem.....	30
3.4.3	Alur Kerja Sistem IPS.....	32
3.5	Skema Pengujian	33
BAB IV	35
4.1	Instalasi dan Konfigurasi Sistem IPS	35
4.1.1	Instalasi Snort	35
4.1.2	Instalasi Paket Web Server.....	45
4.1.3	Instalasi Barnyard	48
4.1.5	Instalasi Snorby.....	55

4.1.6	Startup IPS Server.....	59
4.2	Pengujian Sistem NIPS (<i>Testing</i>)	61
4.2.1	Menjalankan NIPS Server	61
4.3	Pengujian Serangan.....	64
4.3.3	Proses Pengujian Sistem	65
BAB V	79
5.1	Kesimpulan.....	79
5.2	Saran.....	79
DAFTAR PUSTAKA	81
LAMPIRAN	83



DAFTAR TABEL

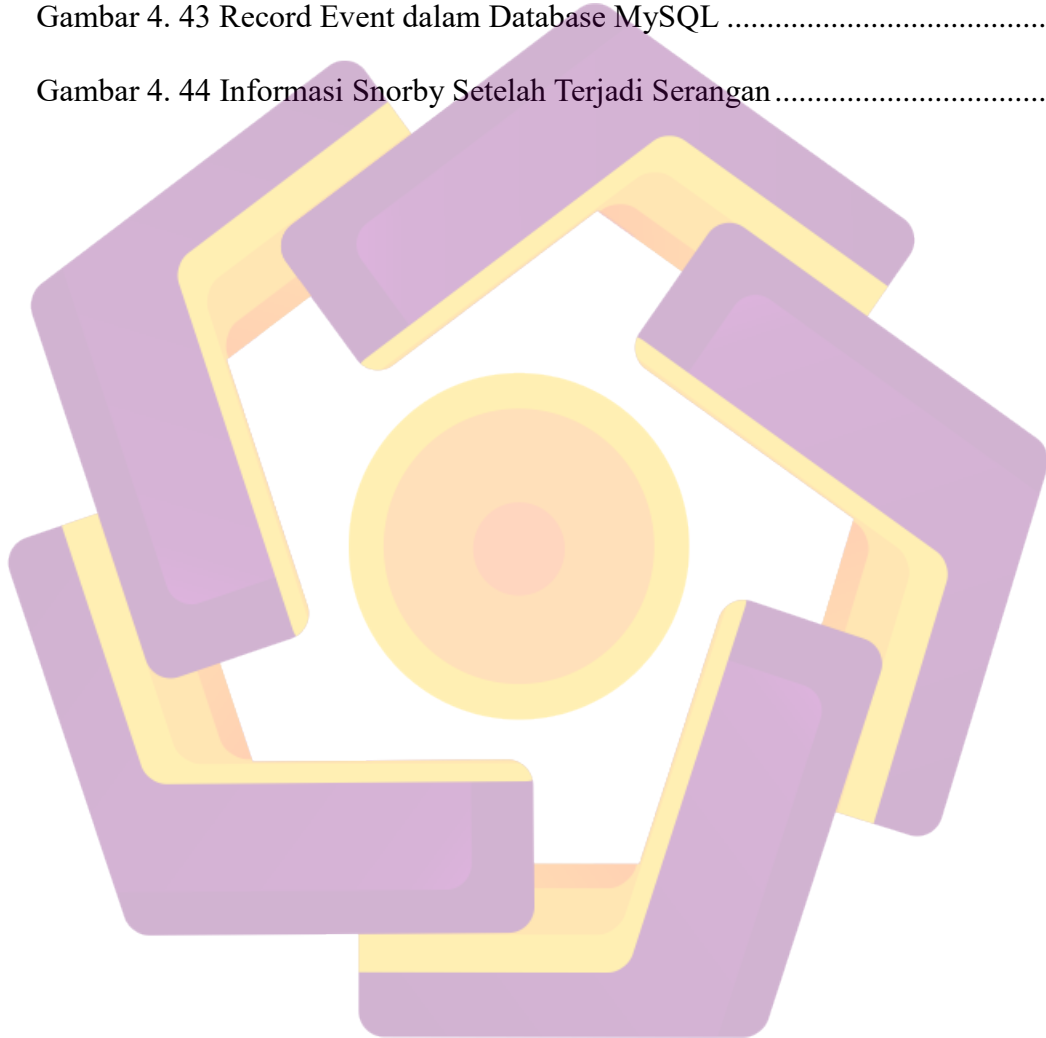
Tabel 2. 1	Klasifikasi Default Snort.....	19
Tabel 2. 2	Simbol-simbol Flowchart.....	21
Tabel 3. 1	Spesifikasi Komputer IPS	27
Tabel 3. 2	Spesifikasi Laptop Attacker	27
Tabel 3. 3	Spesifikasi Laptop Client	28
Tabel 3. 4	Spesifikasi Router Mikrotik	28
Tabel 4. 1	Direktori path dan keterangan	39
Tabel 4. 2	Penggunaan perintah snort	44
Tabel 4. 3	Tabel Pengujian	64
Tabel 4. 4	Penggunaan perintah	67
Tabel 4. 5	Penggunaan perintah hping3	69
Tabel 4. 6	Penggunaan perintah hping3	72
Tabel 4. 7	Daftar Perangkat Lunak yang digunakan.....	77
Tabel 4. 8	Listing Kebutuhan Fungsional	78

DAFTAR GAMBAR

Gambar 2. 1 Hubungan antar komponen snort	16
Gambar 3. 1 Grafik laporan insiden tahun 2016	23
Gambar 3. 2 Grafik jenis serangan DDoS.....	24
Gambar 3.3 Rancangan Topologi penerapan IPS Server	30
Gambar 3. 4 Diagram Hubungan Antar Modul.....	31
Gambar 3. 5 Alur kerja sistem IPS	32
Gambar 3. 6 Rencana Skema Pengujian Sistem IPS	33
Gambar 4. 1 Instalasi Data Acquisition.....	36
Gambar 4. 2 Hasil instalasi snort	37
Gambar 4. 3 Struktur Direktori File Kofigurasi Snort	38
Gambar 4. 4 Hasil Duplikasi file Konfigurasi Snort.....	38
Gambar 4. 5 Struktur Direktori File Kofigurasi Snort.....	39
Gambar 4. 6 Tes Konfigurasi File Snort Sukses	41
Gambar 4. 7 Sebelum dibuat local rules	42
Gambar 4. 8 Sesudah dibuat local rules	43
Gambar 4. 9 Alert ICMP Event.....	44
Gambar 4. 10 Tes Apache melalui browser.....	45
Gambar 4. 11 PHP telah terinstal.....	45
Gambar 4. 12 MySQL telah terinstal	46
Gambar 4. 13 Tampilan halaman Login PhpMyAdmin	47
Gambar 4. 14 Tampilan Dashboard setelah login	47
Gambar 4. 15 Pembuatan tabel dari skema database barnyard.....	50

Gambar 4. 16 Konfigurasi barnyard2.conf	50
Gambar 4. 17 Pulledpork terinstall dengan sukses	51
Gambar 4. 18 Download rules dengan pulledpork selesai	53
Gambar 4. 19 Penambahan rule path	54
Gambar 4. 20 Snort rules berhasil dikonfigurasi	54
Gambar 4. 21 Daily update pulledpork	55
Gambar 4. 22 Tampilan Halaman Login Snorby	58
Gambar 4. 23 Tampilan Dashboard Snorby	58
Gambar 4. 24 Status startup snort sudah aktif	60
Gambar 4. 25 Status startup barnyard2 sudah aktif	61
Gambar 4. 26 Snort sudah Berjalan	62
Gambar 4. 27 Barnyard sudah berjalan.....	63
Gambar 4. 28 Snorby sudah berjalan	64
Gambar 4. 29 Ujicoba konektifitas client dengan server	66
Gambar 4. 30 Respon sistem NIPS terhadap ping test	66
Gambar 4. 31 Portscan menggunakan Nmap	67
Gambar 4. 32 Tampilan alert setelah NIPS dijalankan	68
Gambar 4. 33 Reaksi NIPS terhadap scanning	68
Gambar 4. 34 Denial of Service menggunakan hping3	69
Gambar 4. 35 Hasil capture packet saat terjadi serangan.....	70
Gambar 4. 36 Dampak dari Serangan DoS	70
Gambar 4. 37 Sistem memblock serangan.....	71
Gambar 4. 38 Respon sistem yang terekam	71

Gambar 4. 39 Percobaan Akses SSH	73
Gambar 4. 40 Respon sistem terhadap SSH attack	73
Gambar 4. 41 List snort log file	74
Gambar 4. 42 Contoh isi dari file unified	74
Gambar 4. 43 Record Event dalam Database MySQL	75
Gambar 4. 44 Informasi Snorby Setelah Terjadi Serangan	76



INTISARI

Didalam suatu jaringan komputer tidak semua pengguna yang melakukan akses adalah pengguna legal, terdapat pengguna yang tidak memiliki hak akses berusaha mendapatkan informasi secara ilegal, bahkan tidak sedikit untuk melakukan percobaan serangan terhadap jaringan komputer.

Dalam proses pengamanan sistem keamanan jaringan selalu mengandalkan kinerja seorang *administrator* jaringan. Hal tersebut dapat menyebabkan ketergantungan pada kecepatan dan ketepatan kinerja *administrator* jaringan, maka salah satu metode yang dapat membantu seorang *administrator* jaringan adalah menggunakan Network-based IPS (NIPS).

Network-based IPS (NIPS), yang juga disebut sebagai “*In-line proactive protection*”, menahan semua trafik jaringan dan menginspeksi kelakuan dan kode yang mencurigakan dan merupakan sebuah system yang menerapkan sebuah kebijakan kontrol akses yang memeriksa trafik data dan memblok paket data yang tidak sesuai dengan kebijakan keamanan. Sistematika IPS yang berbasis *signature* adalah dengan cara mencocokkan lalu lintas jaringan dengan *signature* database milik IPS berisi *attacking rule* atau cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Dengan metode pencocokan *signature* ini dapat mengurangi *false positive rate*, dan *rate true positive* lebih tinggi untuk mendeteksi serangan yang akan terjadi.

ABSTRACT

In a computer network, not all users who access are legal users, there are users who do not have access rights trying to get information illegally, not even a few are trying to attack computer networks.

In the process of securing network security systems always rely on the performance of a network administrator. This can lead to dependence on the speed and accuracy of network administrator performance, so one method that can help a network administrator is to use Network-based IPS (NIPS).

Network-based IPS (NIPS), also known as “In-line proactive protection”, blocks all network traffic and inspects suspicious code and behavior and is a system that implements an access control policy that checks data traffic and blocks incoming data packets. Signature-based IPS systematics is by matching network traffic with IPS signature databases containing attacking rules or methods of attack and infiltration that are often carried out by attackers. With this signature matching method, the false positive rate can be reduced, and the true positive rate is higher to detect an imminent attack.