

**ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN
MENGUNAKAN INTRUSION DETECTION SYSTEM DAN FIREWALL**

(Studi Kasus: PT. Sujama Jaya Makmur)

SKRIPSI



disusun oleh

**Abid Aji Prayoga
16.11.0656**

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

2020

**ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN
MENGUNAKAN INTRUSION DETECTION SYSTEM DAN FIREWALL**

(Studi Kasus: PT. Sujama Jaya Makmur)

SKRIPSI

untuk memenuhi sebagian
persyaratan mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

**Abid Aji Prayoga
16.11.0656**

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

2020

PERSETUJUAN

SKRIPSI

ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN MENGUNAKAN INTRUSION DETECTION SYSTEM DAN FIREWALL

(Studi Kasus: PT. Sujama Jaya Makmur)

yang dipersiapkan dan disusun oleh

Abid Aji Prayoga

16.11.0656

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 6 November 2020

Dosen Pembimbing,

Mulia Sulistiyono, M.kom.

NIK. 190302248

**PENGESAHAN
SKRIPSI**

**ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN
MENGUNAKAN INTRUSION DETECTION SYSTEM DAN FIREWALL**

(Studi Kasus: PT. Sujama Jaya Makmur)

yang dipersiapkan dan disusun oleh

**Abid Aji Prayoga
16.11.0656**

telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Maret 2020

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Mulia Sulistiyono, M.Kom

NIK. 190302248

Joko Dwi Santoso, M.Kom

NIK. 190302181

Ferry Wahyu Wibowo, S.Si, M.Cs

NIK. 190302235

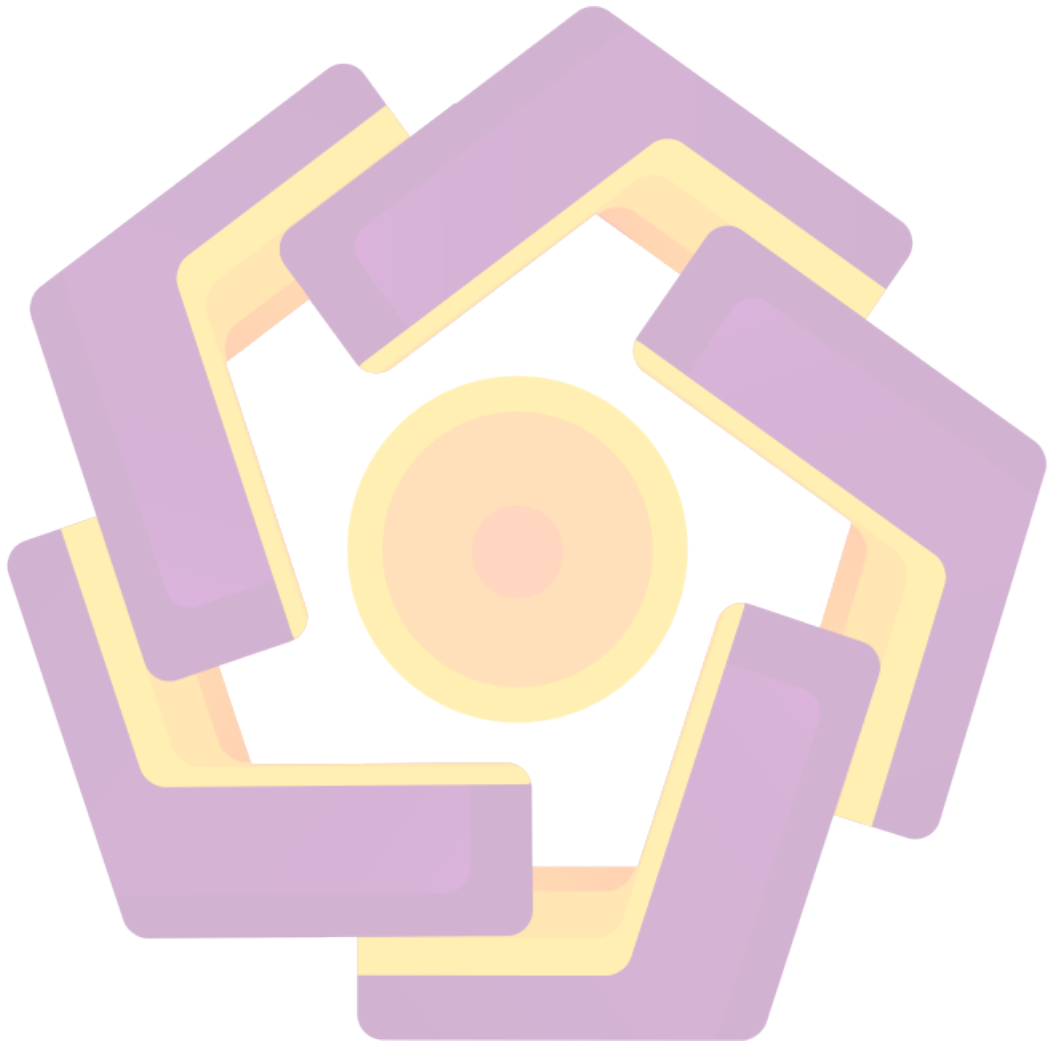
Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 10 Juli 2020

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.

NIK. 190302038

PERNYATAAN



MOTTO

”Sebaik-baiknya motivasi adalah do’a Orang Tua”

Wise Man

“You are free to do everything you want in life, but you must also know that life is very valuable. Think to have a long and stable life”

Melting Me Softly

” Conditions might be choppy, but that won't stop me.”

Morphling Dota 2

“Kuat Dilakoni, Nek Ra Kuat Ditinggal Ngopi”

Nella Kharisma

PERSEMBAHAN

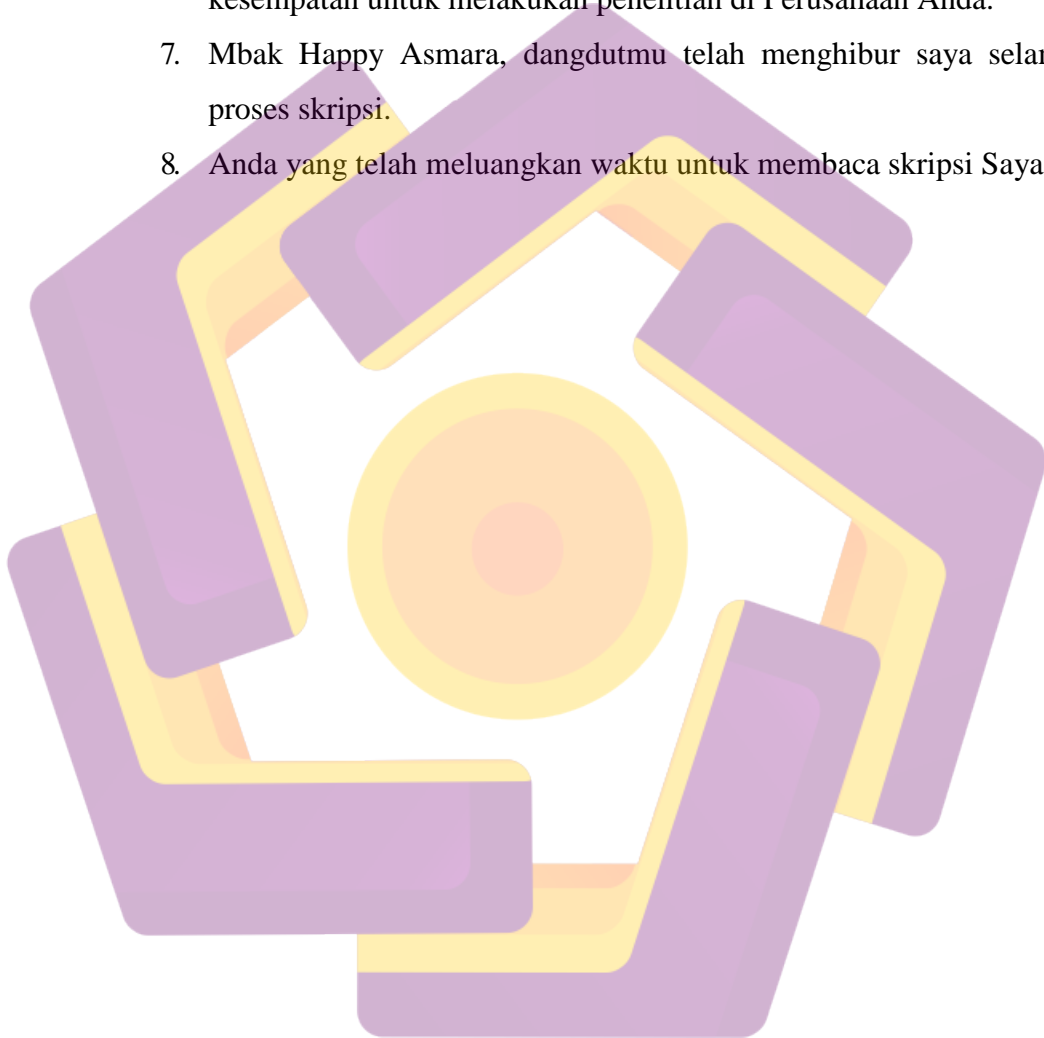
Alhamdulillahirabbil`alamin.

Segala puji bagi Allah SWT Tuhan Semesta Alam atas berkah, rahmat dan hidayah-Nya untuk kelancaran penulisan ini dan juga waktu serta kesempatan untuk merasakan indahny kehidupan. Junjungan besar Nabi Muhammad SAW yang telah menjadi suri tauladan bagi Saya dalam menjalani hidup.

Perjalanan selama lebih dari 3 tahun telah mencapai tahap ini, tahap dimana saya berhasil naik satu tingkat dalam jenjang akademik. Pencapaian ini tidak lepas dari dukungan dan panjatan doa dari orang-orang luar biasa yang berada di sekeliling Saya tentunya. Dengan bangga dan tidak mengurangi rasa hormat serta terimakasih, karya ini Saya persembahkan kepada:

1. Bapak Rajimun dan Ibu Sukarni atas doa-doanya, perjuangan, kasih sayang dan dedikasinya. Karya ini mungkin salah satu perwakilan dari Saya atas perjuangan Bapak dan Ibu selama ini. Mungkin tidak sebanding dengan apa yang telah Bapak dan Ibu berikan kepada Saya.
2. Saudara yang Saya sayangi Mas Rizki, Dzani dan Aan. Karena kalian adalah penyemangat agar bisa menuntaskan karya ini.
3. Pemain DOTA 2 Maguwo e-sport serta Rekan-rekan kontrakan: Monox, Nando, Fajar Pajok, Gondit, Bang Ipenk, Bang Rida, Bang Panji, Bang Edit, Gerot, Bang Farid, Mbak Nur, Mas Papa, Nong Vicky, Mas Juna, Mas Mamik, Mas Tuwek, Mas Ambon, Imam Demang, Mbak Vicka, Mas Unun, Mas Ucup, Bapak Isha, Bang Kevin Jo, Kak Octa dan Keponakan Saya yang imut Ibnu Khalid. Terima Kasih telah menemani Saya selama di Kontrakan.

4. Rekan-rekan Rose House yang telah memberikan dukungan penuh terhadap skripsi Saya.
5. Teman-teman kelas 16 Informatika 10 yang telah bersama-sama berjuang.
6. Dirut PT.Sujama Jaya Makmur, Rida Purwanto telah memberikan kesempatan untuk melakukan penelitian di Perusahaan Anda.
7. Mbak Happy Asmara, dangdutmu telah menghibur saya selama proses skripsi.
8. Anda yang telah meluangkan waktu untuk membaca skripsi Saya.



KATA PENGANTAR

Segala puji syukur dipanjatkan kehadirat Allah SWT atas limpah rahmat hidayah-Nya penulis dapat menyusun skripsi yang berjudul “Analisis Dan PerancanganKeamanan Jaringan Menggunakan Intrusion Detection System Dan Firewall”

Penulis mengucapkan terimakasih kepada semua pihak yang telah memberikan bantuan dan dukungan dalam penyusunan skripsi ini, secara khusus , mengucapkan terimakasih penulis sampaikan kepada :

1. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Universitas AMIKOM Yogyakarta.
2. Bapak Sudarmawan, MT selaku ketua jurusan Teknik Informatika Universitas AMIKOM Yogyakarta.
3. Bapak Mulia Sulistiyono, M.Kom selaku wali sekaligus pembimbing yang telah memberikan dukungan dan motivasi.
4. Bapak Joko Dwi Santoso M.Kom dan Ferry Wahyu Wibowo, S.Si, M.Cs selaku penguji skripsi Saya.
5. Bapak Ibu dosen, staff dan karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu dan bantuannya yang sangat bermanfaat.
6. Kedua orang tua beserta keluarga yang senantiasa memberikan dukungan, kasih sayang serta doa.

DAFTAR ISI

PERSETUJUAN	II
PENGESAHAN	III
PERNYATAAN.....	IV
MOTTO	V
PERSEMBAHAN	VI
KATA PENGANTAR	VIII
DAFTAR ISI.....	IX
DAFTAR TABEL.....	XIII
DAFTAR GAMBAR	XIV
INTISARI.....	XVII
ABSTRACT.....	XVIII
BAB I PENDAHULUAN	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH	3
1.3 BATASAN MASALAH.....	3
1.4 MAKSUD DAN TUJUAN PENELITIAN	4
1.5 MANFAAT PENELITIAN.....	4
1.6 METODE PENELITIAN	4
1.7 SISTEMATIKA PENULISAN	5
BAB II LANDASAN TEORI.....	7
2.1 TINJAUAN PUSTAKA.....	7
2.2 PENGERTIAN ANALISIS SISTEM	12
2.3 PENGERTIAN DESIGN	12
2.4 DEFINISI JARINGAN KOMPUTER	12
2.5 JENIS JARINGAN KOMPUTER	13
2.5.1 Local Area Network.....	13
2.5.2 Metropolitan Area Network	13
2.5.3 Wide Area Network	13
2.6 INTRANET.....	14

2.7	ETHERNET 802.3	14
2.8	PROTOKOL	14
2.9	REFERENSI MODEL OSI	15
2.10	REFERENSI MODEL DOD (TCPIP).....	15
2.10.1	Layer 4 Application.....	16
2.10.2	Layer 3 Transport.....	16
2.10.3	Layer 2 Internet.....	16
2.10.4	Layer 1 Network Interface	16
2.11	IP ADDRESS	17
2.12	JENIS KONEKSI ANTAR JARINGAN KOMPUTER.....	18
2.12.1	Peer To Peer	18
2.12.2	Client Server.....	18
2.13	KEAMANAN KOMPUTER.....	18
2.14	KEBIJAKAN KEAMANAN JARINGAN.....	19
2.15	ASPEK-ASPEK KEAMANAN JARINGAN	20
2.15.1	Interupsi/Interruption.....	20
2.15.2	Intersepsi/Interception.....	20
2.15.3	Modifikasi/Modification	21
2.15.4	Fabrikasi/Fabrication.....	21
2.16	INTRUSION DETECTION SYSTEM	22
2.17	TIBE INTRUSION DETECTION SYSTEM	23
2.17.1	Host Based	23
2.17.2	Network Based.....	23
2.18	PENDEKATAN INTRUSION DETECTION SYSTEM.....	24
2.18.1	Signature Based/Rule Based Detection.....	24
2.18.2	Anomaly Based/Adaptive Detection.....	24
2.19	PASSIVE INTRUSION DETECTION SYSTEM	25
2.20	REACTIVE INTRUSION DETECTION SYSTEM	25
2.21	ARSITEKTUR INTRUSION DETECTION SYSTEM	25
2.21.1	Host Target Co-Location.....	26

2.21.2	Host Target Separation.....	26
2.22	PENGENDALIAN INTRUSION DETECTION SYSTEM.....	26
2.22.1	Terpusat.....	26
2.22.2	Terdistribusi Parsial	26
2.22.3	Terdistribusi Total.....	26
2.23	WAKTU	27
2.23.1	Realtime (Continues).....	27
2.23.2	Interval Based (Batch Mode)	27
2.24	MIKROTIK	27
2.25	FIREWALL	27
2.26	PORT	28
2.27	PPDIOO	29
BAB III ANALISIS DAN PERANCANGAN SISTEM		30
3.1	GAMBARAN UMUM	30
3.2	TAHAP PERSIAPAN (<i>PREPARE</i>).....	31
3.2.1	Analisis Masalah	31
3.2.2	Identifikasi Masalah.....	33
3.2.3	Hipotesis Solusi.....	33
3.3	TAHAP PERENCANAAN (<i>PLAN</i>)	34
3.3.1	Analisis Kebutuhan	35
3.3.2	Kebutuhan Fungsional	35
3.3.3	Kebutuhan Non-Fungsional	35
3.4	DESIGN DAN PERANCANGAN SISTEM (<i>DESIGN</i>).....	39
3.4.1	Rancangan Intrusion Detection System	39
3.4.2	Gambaran Umum Sistem	40
3.4.3	Rancangan Alur Kerja IDS	40
3.4.4	Topologi Implementasi IDS.....	42
3.4.5	Prosedur Implementasi IDS	43
3.4.6	Proses Pendeteksian Serangan	43
3.4.7	Proses Sistem Keseluruhan	44

3.4.8	Prosedur Penjadwalan	45
3.4.9	Perancangan Penempatan Pada Jaringan	46
3.4.10	Perancangan Rule Firewall	46
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	48
4.1	IMPLEMENTASI (<i>IMPLEMENT</i>)	48
4.2	IMPLEMENTASI TOPOLOGI SISTEM	48
4.3	INSTALASI	49
4.3.1	Instalasi Winbox.....	49
4.4	KONFIGURASI.....	49
4.4.1	Konfigurasi System Tool	49
4.4.2	Konfigurasi IDS	55
4.5	TAHAP PENGOPERASIAN (<i>OPERATE</i>).....	66
4.5.1	Fungsionalitas Test.....	67
4.5.2	Respons Time	79
4.6	IDENTIFIKASI.....	83
4.6.1	Masalah Teknis	83
4.6.2	Masalah Non Teknis	84
4.7	PENGOPTIMALAN SISTEM(<i>OPTIMIZE</i>)	84
4.8	EVALUASI SISTEM.....	84
BAB V	PENUTUP.....	86
5.1	KESIMPULAN.....	86
5.2	SARAN.....	87
	DAFTAR PUSTAKA	89
	LAMPIRAN.....	92
	HASIL WAWANCARA DAN OBSERVASI.....	100

DAFTAR TABEL

Tabel 2. 1 Tabel Literatur Review dan Posisi Penelitian.....	9
Tabel 2. 2 IP Address Classfull.....	17
Tabel 3. 1 IP Address Pada Modem ADSL	31
Tabel 3. 2 Spesifikasi Laptop yang dibutuhkan	36
Tabel 3. 3 Spesifikasi Routerboard Mikrotik RB941-2nD-TC.....	37
Tabel 4. 1 Respon Time Serangan Berurutan FTP Bruteforce	80
Tabel 4. 2 Respon Time Serangan Bersamaan FTP Bruteforce.....	81
Tabel 4. 3 Respon Time Serangan Berurutan SSH Bruteforce.....	81
Tabel 4. 4 Respon Time Serangan Bersamaan SSH Bruteforce	81
Tabel 4. 5 Respon Time Serangan Berurutan ICMP Flood.....	82
Tabel 4. 6 Respon Time Serangan Bersamaan ICMP Flood	82
Tabel 4. 7 Respon Time Serangan Berurutan Port Scanning.....	82
Tabel 4. 8 Respon Time Serangan Bersamaan Port Scanning.....	83
Tabel 4. 9 Evaluasi Sistem dan Konfigurasi	84
Tabel 4. 10 Evaluasi Pengujian Sistem	85

DAFTAR GAMBAR

Gambar 2. 1 Referensi Model OSI Layer	15
Gambar 2. 2 Model DOD.....	17
Gambar 2. 3 Interuption	20
Gambar 2. 4 Interception.....	21
Gambar 2. 5 Modification.....	21
Gambar 2. 6 Fabrication.....	22
Gambar 2. 7 Logo Mikrotik	27
Gambar 2. 8 Generic Firewall dan Hardware Firewall	28
Gambar 2. 9 Metode PPDIIO	29
Gambar 3. 1 Topologi Jaringan Lama.....	31
Gambar 3. 2 Routerboard Mikrotik RB941-2nD-TC.....	37
Gambar 3. 3 Gambaran Sistem IDS	40
Gambar 3. 4 Alur Kerja IDS	40
Gambar 3. 5 Topologi Implementasi Jaringan IDS	42
Gambar 3. 6 Flowchart Proses Sistem Keseluruhan	45
Gambar 3. 7 Prosedur Penjadwalan.....	46
Gambar 4. 1 Konfigurasi NTP Client	50
Gambar 4. 2 Konfigurasi Tool Email.....	51

Gambar 4. 3 Uji Coba Pengiriman Pesan Email	52
Gambar 4. 4 Logging Local	53
Gambar 4. 5 Check Rule Firewall FTP	57
Gambar 4. 6 Check rule Firewall SSH.....	60
Gambar 4. 7 Check rule Firewall ICMP Flood	62
Gambar 4. 8 Check rule Firewall Port Scanning.....	64
Gambar 4. 9 Skenario Pengujian Serangan.....	66
Gambar 4. 10 Tampilan Aplikasi BrutusAET-2	68
Gambar 4. 11 Uji Coba Serangan FTP Bruteforce	68
Gambar 4. 12 Log FTP Bruteforce pada Router	69
Gambar 4. 13 Serangan FTP Bruteforce Gagal	70
Gambar 4. 14 Email Report FTP Bruteforce	70
Gambar 4. 15 Address-List FTP Bruteforce	71
Gambar 4. 16 Tampilan awal Aplikasi Putty	71
Gambar 4. 17 SSH Bruteforce Berhasil	72
Gambar 4. 18 Log SSH Bruteforce Pada Router	72
Gambar 4. 19 SSH Bruteforce Gagal.....	73
Gambar 4. 20 Email Report SSH Brutefoce	73
Gambar 4. 21 Address-list SSH Bruteforce	74

Gambar 4. 22 ICMP Flood saat firewall disable.....	74
Gambar 4. 23 Statistik ICMP Flood Bruffer Size 60000.....	75
Gambar 4. 24 ICMP Flood Gagal	75
Gambar 4. 25 Ping yang diizinkan.....	76
Gambar 4. 26 Total Size Ping 32 Byte.....	76
Gambar 4. 27 Laporan Email ICMP Flood.....	77
Gambar 4. 28 IP address-list ICMP FLOOD.....	77
Gambar 4. 29 Tampilan awal Tool Nmap/Zenmap	78
Gambar 4. 30 Uji Coba Serangan Port Scanning.....	78
Gambar 4. 31 Address-list Port Scanning.....	79
Gambar 4. 32 Log Peringatan Port Scanning.....	79
Gambar 4. 33 Laporan Email Serangan Port Scanning.....	79

INTISARI

Sistem keamanan jaringan menjadi sangat penting dalam memelihara jaringan, serangan yang dapat mengganggu dan bahkan merusak sistem koneksi antar perangkat yang terhubung akan sangat berbahaya. Untuk mendapatkan keamanan dalam jaringan kadang-kadang kita harus merasakan ketidaknyamanan dalam penggunaannya, ini sering menjadi pertimbangan dalam penerapan sistem keamanan jaringan di Kantor PT. Sujama Jaya Makmur

WIDS (*Wireless Intrusion Detection System*) mampu mendeteksi serangan DOS (*Denial of Service*), *Ping of Death*. Sistem bekerja dengan mendeteksi serangan dan memberikan peringatan kepada administrator saat mogok.

Pengujian sistem dilakukan dengan menggunakan beberapa jenis serangan ke jaringan untuk dapat mengetahui fungsi sistem bekerja, dengan memberikan laporan dalam bentuk pesan teks yang dikirim pada telepon administrator yang berisi informasi, yaitu alamat IP penyerang dan jenis serangan. Dengan sistem ini, administrator dapat membantu dalam memonitor jaringan.

Keyword: *IDS, Firewall, Network, Security, Administrator.*

ABSTRACT

Network security system becomes very important in maintaining a network, attacks that can interfere and even damage the connection system between devices connected will be very harmful. To gain security in a network sometimes we have to feel the discomfort in its use, this is often a consideration in the application of a network security system in the Sujama Jaya Makmur Office.

WIDS (Wireless Intrusion Detection System) is capable of detecting DOS attacks (Denial of Service), Ping of Death. System works by detecting attacks and to give warning to the administrator when a strike.

Testing the system are carried out using some kind of attack to the network to be able to know the function of the system works, by giving report in the form of a text message sent on the administrator's phone that contains the informations, that are IP address of the attacker and the type of attack. With this system, administrator can be helpful in monitoring the network.

Keyword: *IDS, Firewall, Network, Security, Administrator.*