

**ANALISIS DAN PERANCANGAN INTRUSION DETECTION SYSTEM
MENGUNAKAN MIKROTIK BERBASIS
SMS GATEWAY DAN MAIL REPORT
(Studi Kasus : undukunduk.net Wireless Internet Service)**

SKRIPSI



disusun oleh

Totok Tri Harjanto

11.11.5433

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

**ANALISIS DAN PERANCANGAN INTRUSION DETECTION SYSTEM
MENGUNAKAN MIKROTIK BERBASIS**

SMS GATEWAY DAN MAIL REPORT

(Studi Kasus : undukunduk.net Wireless Internet Service)

SKRIPSI

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



disusun oleh

Totok Tri Harjanto

11.11.5433

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

PERSETUJUAN

SKRIPSI

**ANALISIS DAN PERANCANGAN INTRUSION DETECTION
SYSTEM MENGGUNAKAN MIKROTIK BERBASIS
SMS GATEWAY DAN MAIL REPORT
(Studi Kasus : undukunduk.net Wireless Internet Service)**

yang dipersiapkan dan disusun oleh

Totok Tri Harjanto

11.11.5433

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 30 April 2014

Dosen Pembimbing,



Sudarmawan, MT

NIK. 190302035

PENGESAHAN

SKRIPSI

**ANALISIS DAN PERANCANGAN INTRUSION DETECTION
SYSTEM MENGGUNAKAN MIKROTIK BERBASIS
SMS GATEWAY DAN MAIL REPORT**

(Studi Kasus : undukunduk.net Wireless Internet Service)

yang dipersiapkan dan disusun oleh

Totok Tri Harjanto

11.11.5433

telah dipertahankan di depan Dewan Penguji
pada tanggal 2 September 2015

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Sudarmawan, MT
NIK. 190302035

Dr. Kusrini, M.Kom
NIK. 190302106

Erni Seniwati, M.Cs
NIK. 190302231

Skripsi ini telah diterima sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 3 September 2015

KEJUA STM IK AMIKOM YOGYAKARTA



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

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan hasil 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/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 7 September 2015



Totok Tri Harjanto

11.11.5433

MOTTO

Sesungguhnya bersama kesulitan itu ada kemudahan

Sesungguhnya hanya orang-orang bersabarlah yang dicukupkan pahalanya tanpa batas

Jangan takut untuk bermimpi. Karena mimpi adalah tempat menanam benih harapan dan memetakan cita-cita. Luffy

Hidup adalah pilihan, saat kau tak memilih itu adalah pilihanmu. Luffy



PERSEMBAHAN

Dengan berucap syukur Alhamdulillah, saya persembahkan skripsi ini kepada semua yang telah memberikan doa, dukungan dan bantuan yang tiada hentinya

1. Kedua orang tua saya, Bapak Suyanto dan Ibu Heru Suwarti dan saudara-saudara ku yang selalu mendidik, membimbing saya serta memberikan sarana prasarana, doa dan dukungan dalam menyelesaikan skripsi ini.
2. Lur lur IJO ROYO dan Lur seperjuangan Bobby, Rizal, Vicky, Irfan, Urfa, Laila, Intan, Astri, Ibnu, Jati, Latif, Bangkit, Ita, Riyan, Singgih, Yayan, Vidia, dkk akeh pokoke. Sukses selalu panjang umur. Tetap semangat jangan lupa olahraga.
3. Keluarga besar 11-S1TI-12 yang mulai hilang satu persatu dan yang masih setia bertahan di kampus ungu. Saya bangga menjadi penghuninya, yang membuat kuliah di STMIK AMIKOM Yogyakarta menjadi luar biasa.
4. Keluarga besar HMJTI (Himpunan Mahasiswa Teknik Informatika) STMIK AMIKOM Yogyakarta, suatu hal yang menyenangkan bisa menjadi penghuni sekre HMJTI kost kedua saya selama kepengurusan.
5. Kampus tercinta STMIK AMIKOM Yogyakarta yang telah menjadi tempat pelarian saya selama ini dalam mencari ilmu dan pengalaman dalam menjalani kehidupan menjadi lebih baik dan baik lagi.
6. Khususon buat Mas Duwi Haryanto. Terimakasih atas bimbingan bantuan tenaga pemikiran waktu dll dalam menyelesaikan tugas negara. Sehat dan sukses selalu.
7. Mas Mafazi Akhmad owner undukuduk.net semoga diberi kesehatan selalu. Lancar rejekinya. Makin sukses bisnisnya.. aamiin.
8. Seluruh warga yang sudah mendoakan dan menyemangati.

KATA PENGANTAR

Assalamualaikum Wr. Wb.

Segala puji syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan segala nikmat-Nya yang tiada terkira sehingga penulis mampu menyelesaikan skripsi yang berjudul “ANALISIS DAN PERANCANGAN INTRUSION DETECTION SYSTEM MENGGUNAKAN MIKROTIK BERBASIS SMS GATEWAY DAN MAIL REPORT (Studi Kasus : undukunduk.net Wireless Internet Service).” Dapat selesai sesuai dengan yang diharapkan.

Skripsi ini disusun guna memenuhi salah satu persyaratan dalam rangka menyelesaikan pendidikan pada program Strata satu (S1) pada Jurusan Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

Dalam menyusun skripsi ini penyusun banyak mendapatkan bantuan dari beberapa pihak. Untuk itu penyusun menyampaikan rasa hormat dan terima kasih kepada :

- 1 Prof. Dr. M. Suyanto, MM., selaku ketua STMIK AMIKOM Yogyakarta.
- 2 Sudarmawan, MT. Selaku Ketua Jurusan S1-TI dan sekaligus dosen pembimbing yang telah membimbing dan memberikan masukan yang membangun.
- 3 Tim penguji dan dosen STMIK AMIKOM Yogyakarta yang selama masa study telah memberikan ilmu yang bermanfaat bagi penulis.
- 4 Mafazi Akhmad selaku owner undukunduk.net yang telah memberikan izin untuk penelitian.
- 5 Teman-teman 11-S1TI-12 angkatan 2011 dan semua pihak yang membantu kelancaran penyusunan skripsi ini.

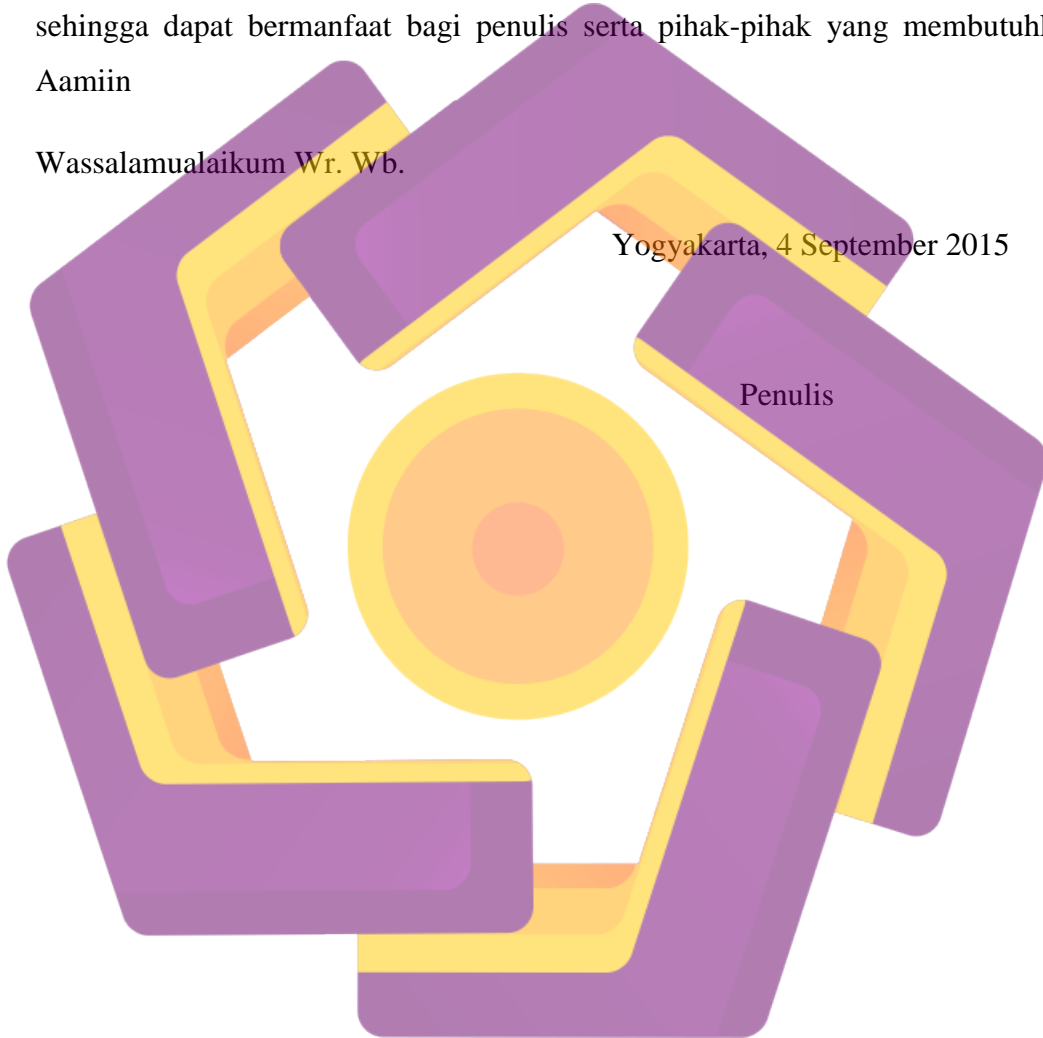
6 Keluarga Besar HMJTI STMIK AMIKOM Yogyakarta yang telah memberikan dukungannya selama ini.

Penulis menyadari masih ada kekurangan dari penyusunan laporan skripsi ini karena keerbatasan penulis dalam hal pengetahuan. Kritik dan saran yang bersifat membangun guna mencapai kesempurnaan skripsi ini selalu penulis harapkan sehingga dapat bermanfaat bagi penulis serta pihak-pihak yang membutuhkan. Aamiin

Wassalamualaikum Wr. Wb.

Yogyakarta, 4 September 2015

Penulis



DAFTAR ISI

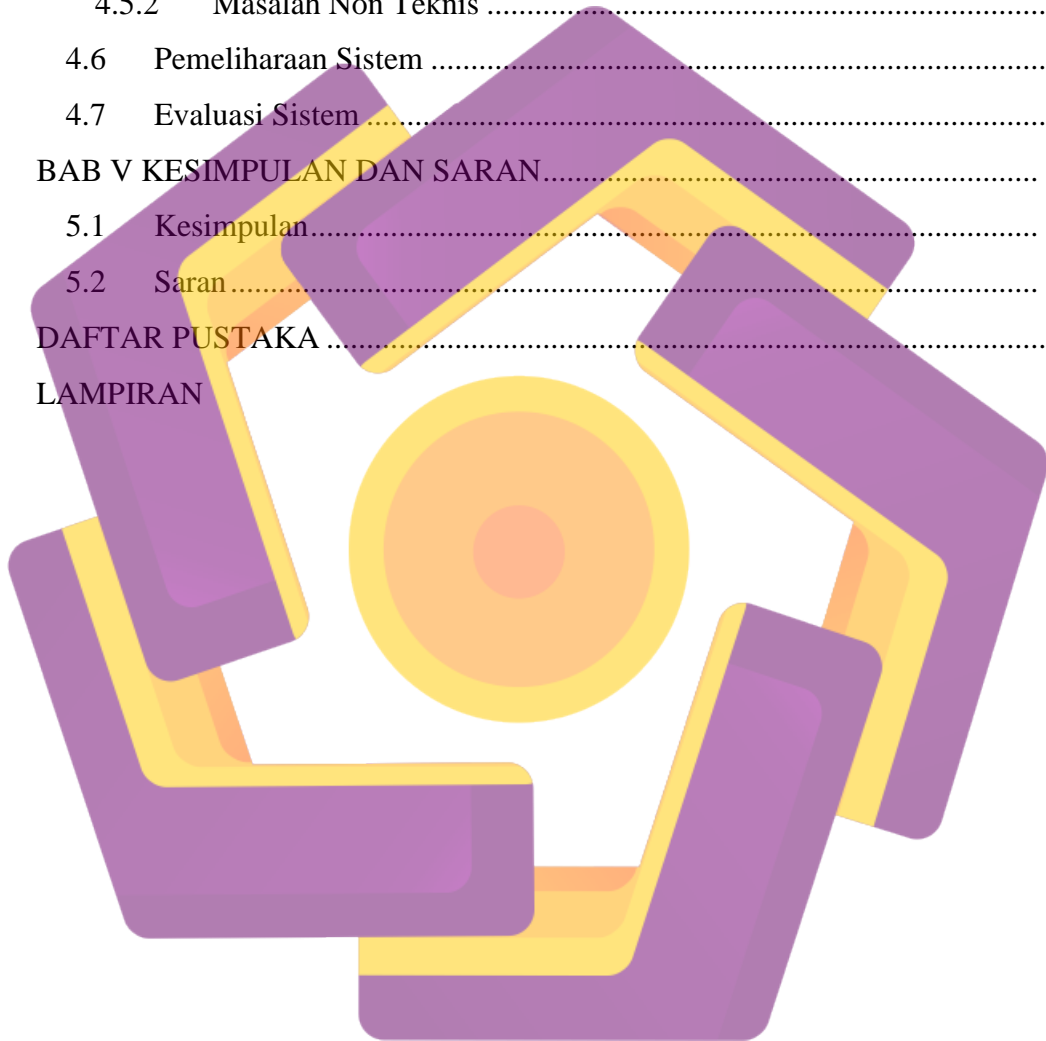
JUDUL	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN.....	iv
MOTTO	v
PERSEMBAHAN.....	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR	xv
DAFTAR LAMPIRAN.....	xviii
INTISARI.....	xix
ABSTRACT.....	xx
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Maksud dan Tujuan	3
1.4.1 Maksud.....	3
1.4.2 Tujuan	3
1.5 Metode Pengumpulan Data	3
1.5.1 Metode Observasi.....	3
1.5.2 Metode Wawancara.....	4
1.5.3 Metode Pustaka	4
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI	8

2.1	Tinjauan Pustaka	8
2.2	Pengertian Analisis Sistem	9
2.3	Pengertian Design.....	9
2.4	Definisi Jaringan Komputer	10
2.6	Jenis Jaringan Komputer	10
2.6.1	Local Area Network.....	10
2.6.2	Metropolitan Area Network	11
2.6.3	Wide Area Network	11
2.8	Intranet.....	11
2.9	Ethernet 802.3	12
2.10	Protokol	12
2.11	Referensi Model OSI.....	12
a.	Layer 7 Application.....	13
b.	Layer 6 Presentation.....	13
c.	Layer 5 Session	13
d.	Layer 4 Transport.....	13
e.	Layer 3 Network.....	13
f.	Layer 2 Data Link.....	13
g.	Layer 1 Physical	13
2.12	Referensi Model DOD (TCP/IP).....	14
2.12.1	Layer 4 Application.....	14
2.12.2	Layer 3 Transport.....	14
2.12.3	Layer 2 Internet	14
2.12.4	Layer 1 Network Interface	15
2.13	IP Address	15
2.14	Jenis Koneksi Antar Jaringan Komputer.....	16
2.14.1	Peer To Peer	16
2.14.2	Client Server.....	16
2.15	Keamanan Komputer.....	17
2.16	Keamanan Informasi	17
2.17	Kebijakan Keamanan Jaringan	18

2.18	Aspek-aspek Keamanan Jaringan.....	18
2.18.1	Interupsi/Interruption.....	18
2.18.2	Intersepsi/Interception.....	19
2.18.3	Modifikasi/Modification	19
2.18.4	Fabrikasi/Fabrication.....	20
2.19	Intrusion Detection System	20
2.20	Tipe Intrusion Detection System	22
2.20.1	Host Based	22
2.20.2	Network Based	22
2.21	Pendekatan Intrusion Detection System	22
2.21.1	Signatur Based/Rule Based Detection	22
2.21.2	Anomaly Based/Adaptive Detection.....	23
2.22	Passive Intrusion Detection System	24
2.23	Reactive Intrusion Detection System	24
2.24	Arsitektur Intrusion Detection System	24
2.24.1	Host Target Co-Location.....	24
2.24.2	Host Target Separation.....	25
2.25	Tujuan Intrusion Detection System.....	25
2.25.1	Tanggung Jawab.....	25
2.25.2	Respon.....	25
2.26	Pengendalian Intrusion Detection System.....	25
2.26.1	Terpusat.....	25
2.26.2	Terdistribusi Parsial	26
2.26.3	Terdistribusi Total.....	26
2.27	Waktu	26
2.27.1	Interval Based (Batch Mode)	26
2.27.2	Realtime (Continues)	26
2.28	Mikrotik.....	26
2.29	Firewall.....	27
2.30	Port	28
2.31	SMS (Short Messege Service).....	28

BAB III ANALISIS DAN PERANCANGAN SISTEM	30
3.1 Gambaran Umum	30
3.1.1 Misi dan Tujuan	31
3.1.2 Topologi Sistem Yang Berjalan.....	31
3.2 Analisis Masalah	32
3.2.1 Sistem Pendeteksi Network Attack.....	32
3.2.2 Laporan Network Attack.....	32
3.2.3 Email Report network Attack	32
3.2.4 Sistem Peringatan Serangan.....	33
3.2.5 Firewall	33
3.3 Hipotesis Solusi.....	33
3.3.1 Intrusion Detection System.....	33
3.4 Analisis Kebutuhan Sistem	34
3.4.1 Analisis Kebutuhan Fungsional	34
3.4.2 Analisis Kebutuhan Non Fungsional	35
3.5 Perancangan Sistem.....	36
3.5.1 Rancangan Intrusion Detection System.....	36
3.5.2 Gambaran Umum Sistem.....	37
3.5.3 Rancangan Alur Kerja IDS	38
3.5.4 Topologi Implementasi IDS.....	40
3.5.5 Prosedur Implementasi IDS	40
3.5.6 Proses Pendeteksian Serangan.....	41
3.5.7 Proses Sistem Keseluruhan	42
3.5.8 Prosedur Penjadwalan	43
3.5.9 Perancangan Penempatan Pada Jaringan	44
3.5.10 Perancangan Rule Firewall	45
BAB IV IMPLEMENTASI DAN PEMBAHASAN	46
4.1 Implementasi	46
4.2 Implementasi Topologi Sistem.....	46
4.3 Instalasi Dan Konfigurasi.....	47
4.3.1 Instalasi	47

4.3.2	Konfigurasi.....	48
4.4	Pembahasan Sistem	70
4.4.1	Pengujian IDS	70
4.5	Identifikasi.....	96
4.5.1	Masalah Teknis	96
4.5.2	Masalah Non Teknis	97
4.6	Pemeliharaan Sistem	97
4.7	Evaluasi Sistem	97
BAB V KESIMPULAN DAN SARAN.....		101
5.1	Kesimpulan.....	101
5.2	Saran.....	102
DAFTAR PUSTAKA		xvi
LAMPIRAN		



DAFTAR TABEL

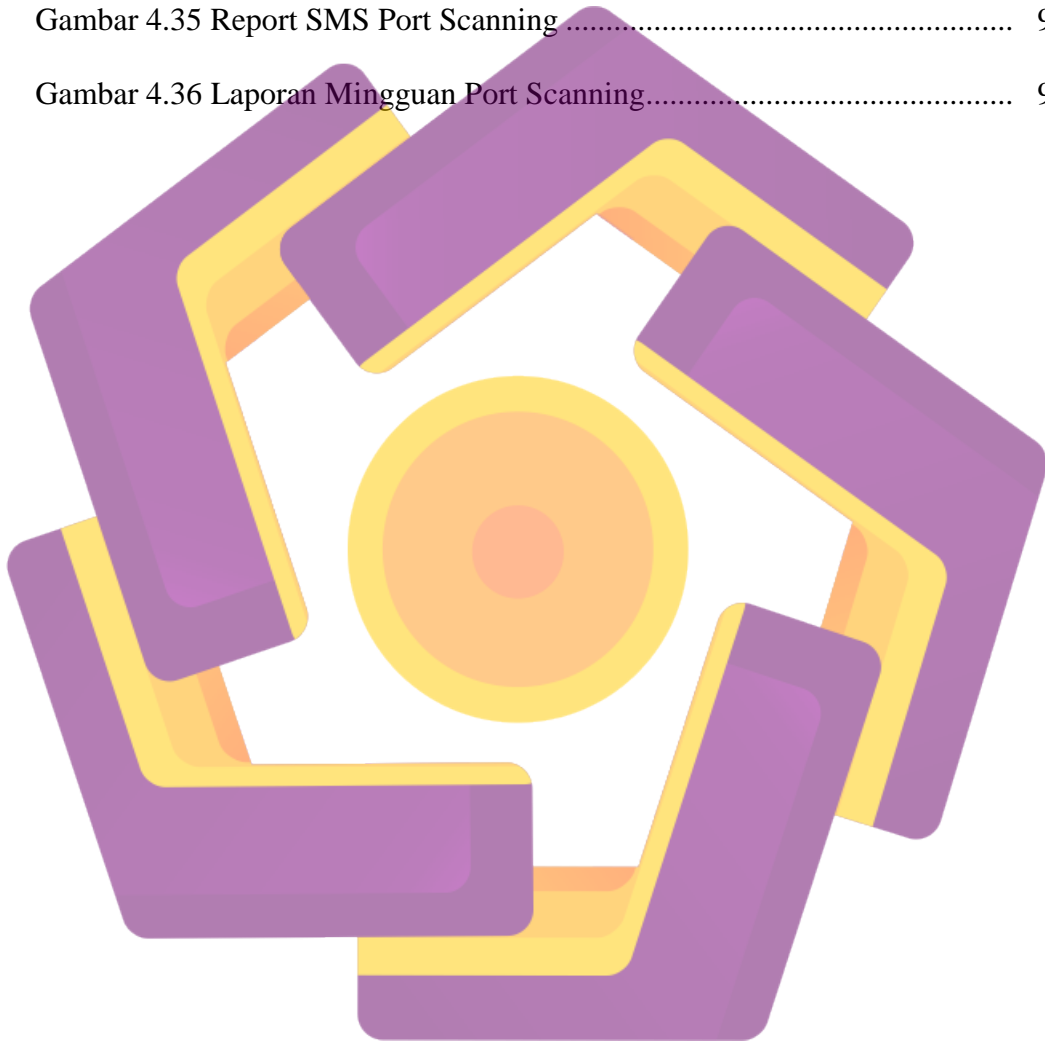
Tabel 2.1 IP Address Classfull.....	15
Tabel 3.1 Kebutuhan Hardware PC Router Mikrotik	35
Tabel 4.1 Respon Time Serangan Berurutan FTP Bruteforce	92
Tabel 4.2 Respon Time Serangan Bersamaan FTP Bruteforce.....	93
Tabel 4.3 Respon Time Serangan Berurutan SSH Bruteforce.....	93
Tabel 4.4 Respon Time Serangan Bersamaan SSH Bruteforce	94
Tabel 4.5 Respon Time Serangan Berurutan ICMP Flood	94
Tabel 4.6 Respon Time Serangan Bersamaan ICMP Flood	94
Tabel 4.7 Respon Time Serangan Berurutan Port Scanning.....	95
Tabel 4.8 Respon Time Serangan Bersamaan Port Scanning	95
Tabel 4.9 Evaluasi Instalasi Dan Konfigurasi.....	98
Tabel 4.10 Evaluasi Pengujian Sistem.....	100

DAFTAR GAMBAR

Gambar 2.1 OSI Layer	13
Gambar 2.2 Model DOD.....	15
Gambar 2.3 Interupsi.....	19
Gambar 2.4 Intersepsi	19
Gambar 2.5 Modifikasi	20
Gambar 2.6 Fabrikasi.....	20
Gambar 2.7 Logo Mikrotik	27
Gambar 2.8 Firewall.....	28
Gambar 3.1 Logo Perusahaan	30
Gambar 3.2 Gambaran Sistem Yang Berjalan	31
Gambar 3.3 Gambaran Umum Sistem	38
Gambar 3.4 Alur Kerja IDS	38
Gambar 3.5 Topologi Implementasi IDS	40
Gambar 3.6 Proses Keseluruhan Sistem	43
Gambar 3.7 Prosedur Penjadwalan	44
Gambar 4.1 Konfigurasi NTP Client	49
Gambar 4.2 Konfigurasi Tool Email Pada Winbox	50
Gambar 4.3 Uji Coba Pengiriman Pesan Email	50
Gambar 4.4 Logging Local	52
Gambar 4.5 Skenario Serangan.....	71
Gambar 4.6 Tampilan Aplikasi BrutusA2	72
Gambar 4.7 Uji Coba Serangan FTP Bruteforce	73

Gambar 4.8 Log FTP Bruteforce Pada Router.....	74
Gambar 4.9 Serangan FTP Bruteforce Gagal	74
Gambar 4.10 Email Report FTP Bruteforce	75
Gambar 4.11 Report SMS FTP Bruteforce	76
Gambar 4.12 Address List FTP Bruteforce	76
Gambar 4.13 Laporan Mingguan FTP Bruteforce	77
Gambar 4.14 Tampilan Aplikasi Putty.....	78
Gambar 4.15 SSH Bruteforce Berhasil	78
Gambar 4.16 Log SSH Bruteforce Pada Router	79
Gambar 4.17 SSH Bruteforce Gagal.....	79
Gambar 4.18 Email Report Serangan SSH Bruteforce	80
Gambar 4.19 Address List SSH Bruteforce	80
Gambar 4.20 Report SMS SSH Bruteforce	81
Gambar 4.21 Laporan Mingguan SSH Bruteforce.....	82
Gambar 4.22 Serangan ICMP Flood.....	83
Gambar 4.23 Statistik ICMP Flood Buffer Size 65000	83
Gambar 4.24 ICMP Flood Gagal	84
Gambar 4.25 Ping Yang Di Izinkan.....	84
Gambar 4.26 Total Size Ping 32 Byte.....	85
Gambar 4.27 Laporan Email Serangan ICMP FLOOD	85
Gambar 4.28 Report SMS ICMP Flood.....	86
Gambar 4.29 Laporan Mingguan ICMP Flood.....	86
Gambar 4.30 Tampilan Tool Nmap/Zenmap.....	87

Gambar 4.31 Uji Coba Port Scanning.....	88
Gambar 4.32 Address List Port Scanning.....	88
Gambar 4.33 Pesan Peringatan Serangan pada Log Router.....	89
Gambar 4.34 Laporan Email Serangan Port Scanning.....	89
Gambar 4.35 Report SMS Port Scanning.....	90
Gambar 4.36 Laporan Mingguan Port Scanning.....	91



DAFTAR LAMPIRAN

SURAT PERSETUJUAN IJIN PENELITIAN.....	xviii
HASIL WAWANCARA DAN OBSERVASI.....	xix



INTISARI

Kemananan Jaringan pada saat ini sangatlah penting. Meningkatnya jumlah komputer yang terhubung ke internet menjadikan kesenjangan yang rentan pada keamanan jaringan. Administrator memiliki peran penting dalam melindungi keamanan jaringan pada sebuah server. Proses monitoring selama 24 jam merupakan kegiatan yang dilakukan Administrator dalam mengawasi dan melindungi jaringan. Keterbatasan manusiawi seperti lelah, kelalaian, dll merupakan kendala bagi administrator.

Membangun IDS (*Intrusion Detection System*) merupakan salah satu solusi pemecahan masalah tersebut. Sistem ini bekerja dengan cara mendeteksi adanya serangan dan memberikan peringatan kepada administrator jaringan apabila terjadi serangan pada jaringan, selain itu IDS juga dapat digunakan untuk melakukan pengawasan jaringan.

Pengujian sistem ini dilakukan dengan menggunakan beberapa jenis serangan ke jaringan dan pengujian fungsionalitas sistem adalah dengan melakukan cek peringatan dan *report* cepat berupa SMS yang dikirim ke *mobile* administrator dan email yang berisi IP penyerang untuk dikirim ke email administrator, guna membantu administrator dalam melakukan monitoring jaringan.

Kata Kunci : Intrusion Detection System, SMS Gateway, Administrator, Keamanan Jaringan

ABSTRACT

Network security is very important at this time. The increasing number of computers connected to the Internet make vulnerable gaps in network security. Administrators have an important role in protecting the security of the network on a server. Process monitoring for 24 hours is an activity undertaken Administrator in overseeing and protecting the network. Human limitations such as fatigue, negligence, etc. is an obstacle for the administrator.

Build IDS (Intrusion Detection System) is one solution to solving the problem. This system works by detecting an attack and alert the network administrator in case of an attack on the network, in addition to the IDS can also be used for network monitoring.

System testing is performed using several types of attacks to the network and testing the functionality of the system is to do a quick check in the form of alerts and reports are sent to the mobile SMS and email administrator that contains the attacker's IP to be sent to the email administrator, to assist administrators in performing network monitoring.

Keywords: Intrusion Detection System, SMS Gateway, Administrator, Network Security