

**ANALISIS DAN PERANCANGAN REACTIVE INTRUSION  
DETECTION SYSTEM MENGGUNAKAN MIKROTIK  
BERBASIS LOG DAN MAIL REPORT  
(Studi Kasus : PT. Wahana Lintas Nusa Persada)**

**SKRIPSI**



disusun oleh

**Duwi Haryanto**

**10.11.3719**

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

**ANALISIS DAN PERANCANGAN REACTIVE INTRUSION DETECTION  
SYSTEM MENGGUNAKAN MIKROTIK BERBASIS LOG DAN EMAIL  
REPORT**

**(Studi Kasus : PT. Wahana Lintas Nusa Persada)**

**SKRIPSI**

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



disusun oleh

**Duwi Haryanto**

**10.11.3719**

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

# PERSETUJUAN

## SKRIPSI

### ANALISIS DAN PERANCANGAN REACTIVE INTRUSION DETECTION SYSTEM MENGGUNAKAN MIKROTIK BERBASIS LOG DAN MAIL REPORT (Studi Kasus : PT. Wahana Lintas Nusa Persada)

yang dipersiapkan dan disusun oleh

**Duwi Haryanto**

**10.11.3719**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 3 Agustus 2013

**Dosen Pembimbing,**



**Sudarmawan, MT**

**NIK. 190302035**

# PENGESAHAN

## SKRIPSI

### ANALISIS DAN PERANCANGAN REACTIVE INTRUSION DETECTION SYSTEM MENGGUNAKAN MIKROTIK BERBASIS LOG DAN MAIL REPORT

(Studi Kasus : PT. Wahana Lintas Nusa Persada)

yang dipersiapkan dan disusun oleh

**Duwi Haryanto**

**10.11.3719**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 6 Maret 2014

#### Susunan Dewan Penguji

**Nama Penguji**

**Tanda Tangan**

**Sudarmawan, MT**  
**NIK. 190302035**

**Andi Sunyoto, M.Kom**  
**NIK. 190302052**

**Dony Ariyus, S.S, M.Kom**  
**NIK. 190302128**

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 7 Maret 2014

**KEFUA STMIK AMIKOM YOGYAKARTA**



**Prof. Dr. M. Suvanto, 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 Maret 2014

Duwi haryanto  
10.11.3719

## **MOTTO**

“KAU MENCIPTAKAN SEMESTAMU, DISETIAP LANGKAHMU”

“ORANG SUSKSES ADALAH ORANG YANG MELAKUKAN SESUATU  
KARENA MEMANG HARUS DILAKUKAN MESKIPUN ITU TIDAK  
DISUKAINYA”

“INVESTASI YANG PALING MENGUNTUNGAN ADALAH BELAJAR”

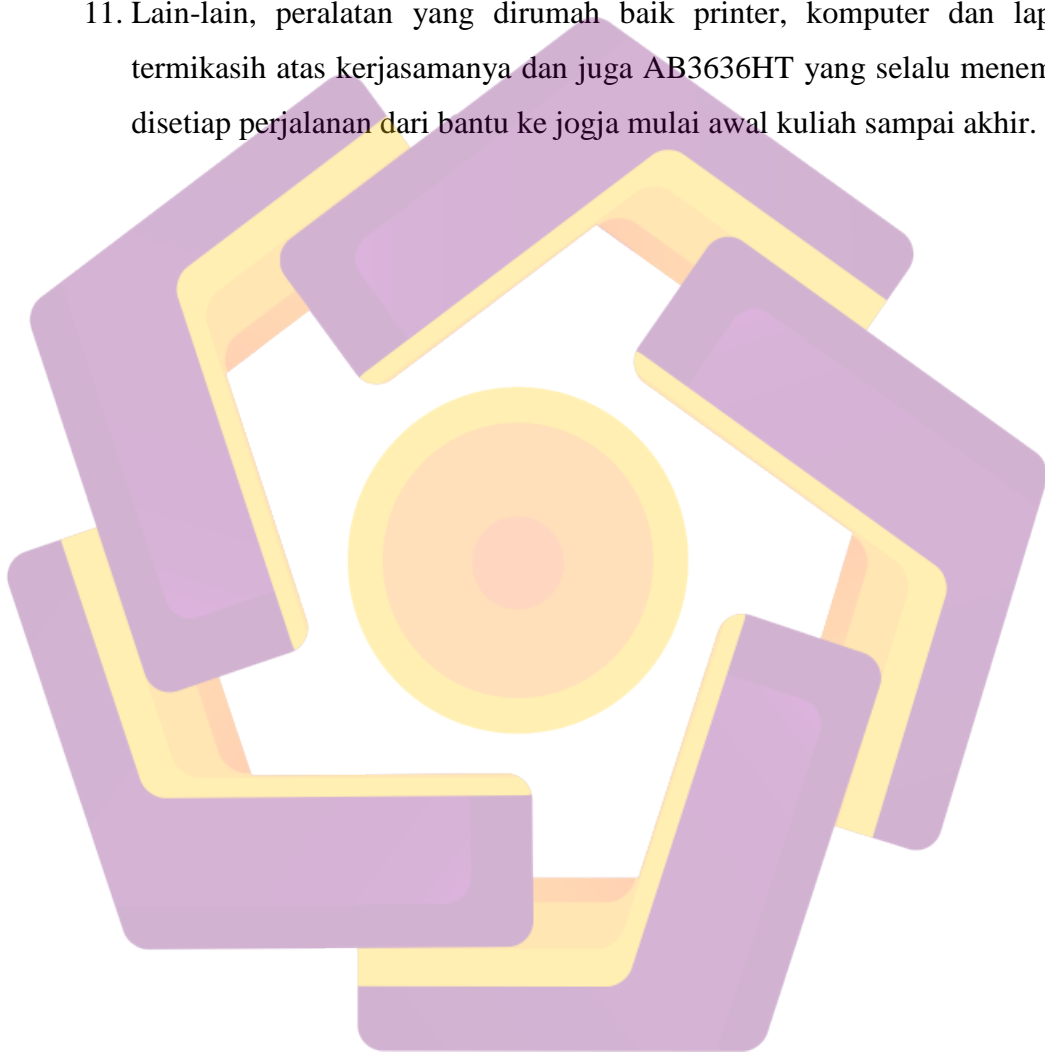


## PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

1. Kedua orang tua saya, Bapak MURDIYONO dan Ibu SARJIYEM yang selalu mendidik, membimbing, melatih dan mengajarkan hal yang baik-baik kepada saya serta memberikan doa dan dukungan dalam menyelesaikan skripsi ini.
2. Kakakku ARIS WIDIYANTO yang telah memfasilitasi saya peralatan yang dibutuhkan serta semangat dan dukungannya untuk menyelesaikan skripsi ini sesuai dengan target yang telah saya tentukan.
3. Adikku TITIK WULANDARI yang telah memberikan semangat dan dukungannya untuk menyelesaikan skripsi ini tepat waktu.
4. Teman kumpul sekaligus sahabat, WAHID HARTOMO, WYLDAN CANDRA A, NOVENTA PUNGKI R, RIDHO ARJI H, ARIFIN, MARZUQI DWI, BAMBANG JATI P, RUDI Y yang selalu kumpul dari semester 1 sampai 7, sehat dan sukses selalu buat kalian.
5. Teman seperjuangan ERWIN, ANGGI, ARDHA, CICI, PITI, TITA, RANDI, FIKRI, AYYAS, YUSRON, IQMAL, PARSIMIN, KOKO, ARIFIN, RIDHO, AZHARI dan GINA pengalaman membuat event bersama kalian tidak akan mudah terlupakan, sukses dan sehat selalu buat kalian.
6. Keluarga besar S1-TI-03, saya bangga menjadi penghuninya, yang membuat kuliah di STMIK AMIKOM Yogyakarta menjadi menyenangkan.
7. Keluarga besar HMJTI (Himpunan Mahasiswa Teknik Informatika) STMIK AMIKOM Yogyakarta, terimakasih atas pengalaman keorganisasiannya dan ilmu tambahannya selama ini, membuat kuliah di STMIK AMIKOM menjadi menantang dan tidak monoton.
8. Kampus tercinta STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmu dan pengalaman dalam menjalani kehidupan menjadi lebih baik dan baik lagi.

9. Warga FMI (Forum Mikrotik Indonesia) yang telah memberikan banyak referensi mengenai tutorial-tutorial mikrotiknya.
10. PT. Wahana Lintas Nusa Persada (WLAN) Yogyakarta yang telah memberikan izin kepada penulis untuk melakukan observasi dan penelitian.
11. Lain-lain, peralatan yang dirumah baik printer, komputer dan laptop termikasih atas kerjasamanya dan juga AB3636HT yang selalu menemani disetiap perjalanan dari bantu ke jogja mulai awal kuliah sampai akhir.





## 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 REACTIVE INTRUSION DETECTION SYSTEM MENGGUNAKAN MIKROTIK BERBASIS LOG DAN EMAIL REPORT (Studi kasus: PT. Wahana Lintas Nusa Persada).” Dapat selesai sesuai dengan target yang telah direncanakan.

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 Ir. Syafiq Iqbal selaku direktur PT.Wahana Lintas Nusa Persada (WLAN) yang telah memberikan izin untuk penelitian.
- 4 Dody, Yogi, Vani dan Kaka beserta seluruh karyawan PT.Wahana Lintas Nusa Persada Yogyakarta yang telah membantu memberi masukan dan saran serta ilmunya dalam mengerjakan skripsi ini.
- 5 Tim penguji dan dosen STMIK AMIKOM Yogyakarta yang selama masa study telah memberikan ilmu yang bermanfaat bagi penulis.
- 6 Keluarga Besar HMJTI STMIK AMIKOM Yogyakarta yang telah memberikan dukungannya selama ini.

7 Teman-teman S1-TI-03 angkatan 2010 dan semua pihak yang membantu kelancaran penyusunan skripsi yang tidak dapat penulis tulis satu persatu.

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.  
Amin

Wassalamualaikum Wr. Wb.

Yogyakarta, 7 Maret 2014



## DAFTAR ISI

<b>JUDUL</b> .....	i
<b>PERSETUJUAN</b> .....	ii
<b>PENGESAHAN</b> .....	iii
<b>PERNYATAAN</b> .....	iv
<b>MOTTO</b> .....	v
<b>PERSEMBAHAN</b> .....	vi
<b>KATA PENGANTAR</b> .....	viii
<b>DAFTAR ISI</b> .....	x
<b>DAFTAR TABEL</b> .....	xvii
<b>DAFTAR GAMBAR</b> .....	xviii
<b>DAFTAR LAMPIRAN</b> .....	xxiii
<b>INTISARI</b> .....	xxiv
<b>ABSTRACT</b> .....	xxv
<b>BAB I</b> .....	1
1.1    Latar Belakang Masalah.....	1
1.2    Rumusan Masalah .....	3
1.3    Batasan Masalah.....	3
1.4    Maksud Dan Tujuan .....	4
1.4.1    Maksud.....	4
1.4.2    Tujuan .....	4
1.5    Manfaat Penelitian.....	4
1.5.1    Bagi Penulis .....	4
1.5.2    Bagi Perusahaan .....	5
1.6    Metode Pengumpulan Data .....	5
1.6.1    Metode Observasi.....	5
1.6.2    Metode Wawancara.....	5
1.6.3    Metode Pustaka .....	6
1.7    Metodelogi Penelitian.....	6

1.8	Sistematika Penulisan.....	8
1.9	Pelaksanaan Kegiatan.....	10
<b>BAB II</b>	.....	11
2.1.	Tinjauan Pustaka .....	11
2.2.	Pengertian Analisis Sistem.....	12
2.3.	Pengertian Design.....	12
2.4.	Definisi Jaringan Komputer .....	13
2.5.	Sejarah Jaringan Komputer .....	13
2.6.	Jenis Jaringan Komputer .....	14
2.6.1	Local Area Network.....	14
2.6.2	Metropolitan Area Network.....	14
2.6.3	Wide Area Network .....	15
2.7.	Topologi Jaringan.....	15
2.7.1	Topologi Star.....	16
2.7.2	Topologi Bus .....	16
2.7.3	Topologi Ring .....	17
2.7.4	Topologi Tree.....	17
2.7.5	Topologi Mesh .....	18
2.7.6	Topologi Hybrid.....	19
2.8	Media Penghantar.....	20
2.8.1	Wire Network.....	20
2.8.2	Wireless Newtork.....	20
2.9	Intranet.....	21
2.10	Ethernet 802.3.....	21
2.11	Protokol.....	21
2.12	Referensi Model OSI .....	22
2.12.1	Layer 7 Aplication.....	22
2.12.2	Layer 6 Presentation.....	22
2.12.3	Layer 5 Session .....	23
2.12.4	Layer 4 Transport.....	23
2.12.5	Layer 3 Network .....	23

2.12.6	Layer 2 Data Link .....	23
2.12.7	Layer 1 Physical.....	24
2.13	Referensi Model DOD (TCP/IP) .....	24
2.13.1	Layer 4 Application.....	25
2.13.2	Layer 3 Transport.....	25
2.13.3	Layer 2 Internet.....	25
2.13.4	Layer 1 Network Interface .....	25
2.14	IP Address.....	26
2.15	Jenis Koneksi Antar Jaringan Komputer .....	27
2.15.1	Peer To Peer .....	27
2.15.2	Client Server.....	27
2.16	Keamanan Komputer .....	27
2.17	Keamanan Informasi.....	28
2.18	Kebijakan Keamanan Jaringan .....	29
2.19	Aspek-aspek Keamanan Jaringan .....	30
2.19.1	Interupsi/Interruption.....	30
2.19.2	Intersepsi/Interception.....	30
2.19.3	Modifikasi/Modification .....	31
2.19.4	Fabrikasi/Fabrication.....	32
2.20	Intrusion Detection System.....	32
2.21	Tipe Intrusion Detection System .....	34
2.21.1	Host Based .....	34
2.21.2	Network Based .....	34
2.22	Pendekatan Intrusion Detection System .....	35
2.22.1	Signatur Based/Rule Based Detection .....	35
2.22.2	Anomaly Based/Adaptive Detection.....	35
2.23	Passive Intrusion Detection System.....	36
2.24	Reactive Intrusion Detection System.....	36
2.25	Arsitektur Intrusion Detection System .....	36
2.25.1	Host Target Co-Location.....	36
2.25.2	Host Target Separation.....	37

2.26	Tujuan Intrusion Detection System .....	37
2.26.1	Tanggung Jawab.....	37
2.26.2	Respon.....	37
2.27	Pengendalian Intrusion Detection System .....	37
2.27.1	Terpusat.....	38
2.27.2	Terdistribusi Parsial .....	38
2.27.3	Terdistribusi Total.....	39
2.28	Waktu.....	40
2.28.1	Interval Based (Batch Mode) .....	40
2.28.2	Realtime (Continues) .....	40
2.29	Mikrotik .....	40
2.29.1	Tool Email.....	41
2.29.2	Log .....	41
2.29.3	Schedule.....	41
2.29.4	Script Repository.....	42
2.30	Firewall.....	42
2.31	Port.....	43
<b>BAB III</b>	.....	44
3.1	Gambaran Umum Perusahaan .....	44
3.1.1	Visi .....	44
3.1.2	Misi .....	45
3.1.3	Struktur Organisasi .....	45
3.2	Analisis Masalah .....	46
3.2.1	Sistem Pendeteksi Network Attack.....	47
3.2.2	Laporan Network Attack.....	47
3.2.3	Email Report Network Attack.....	47
3.2.4	System Logging .....	48
3.2.5	Firewall .....	48
3.2.6	Topologi Jaringan Saat Ini .....	48
3.3	Hipotesis Solusi.....	49
3.3.1	Reactive Intrusion Detection System.....	49

3.3.2	Syslog Server .....	50
3.4	Analisis Kebutuhan Sistem .....	50
3.4.1	Analisis Kebutuhan Fungsional .....	50
3.4.2	Analisis Kebutuhan Non Fungsional .....	52
3.4.2.1	Kebutuhan Hardware.....	52
3.4.2.1.1	Kebutuhan Hardware Mikrotik.....	52
3.4.2.1.2	Kebutuhan Hardware Syslog Server.....	53
3.4.2.2	Kebutuhan Software .....	54
3.4.2.2.1	Kebutuhan Software IDS .....	54
3.4.2.2.2	Kebutuhan Software Percobaan Serangan.....	55
3.4.2.3	Analisis Biaya.....	55
3.4.2.3.1	Kebutuhan Biaya Hardware.....	55
3.4.2.3.2	Kebutuhan Biaya Software .....	56
3.4.2.3.3	Kebutuhan Software Pendukung .....	56
3.4.2.4	Analisis Kebutuhan Brainware.....	57
3.4.2.5	Analisis Manfaat Sistem.....	57
2.5	Perancangan Sistem.....	58
2.5.2	Rancangan Reactive IDS.....	58
2.5.3	Gambaran Umum Sistem .....	59
2.5.4	Rancangan Alur Kerja Reactive IDS .....	61
3.5.4	Topologi Implementasi Reactive IDS.....	62
3.5.5	Prosedur Implementasi Reactive IDS .....	63
3.5.6	Proses Pendeteksian Serangan .....	64
3.5.7	Proses Sistem Keseluruhan .....	65
3.5.8	Prosedur Penjadwalan .....	66
3.5.9	Perancangan Penempatan Pada Jaringan .....	67
3.5.10	Perancangan Rule Firewall .....	68
<b>BAB IV</b>	.....	<b>69</b>
4.1	Implementasi .....	69
4.2	Implementasi Topologi Sistem.....	69
4.3	Instalasi Dan Konfigurasi.....	71

4.3.1	Instalasi .....	71
4.3.1.1	Instalasi Mikrotik Versi 5.20.....	71
4.3.1.2	Instalasi The Dude Versi 4 .....	72
4.3.1.3	Instalasi Mikrotik Syslog.....	73
4.3.1.4	Instalasi Winbox.....	74
4.3.2	Konfigurasi.....	75
4.3.2.1	Konfigurasi System Tool.....	75
4.3.2.1.1	Konfigurasi System Identity .....	76
4.3.2.1.2	Konfigurasi Network Time Protokol .....	77
4.3.2.1.3	Konfigurasi Tool Email .....	79
4.3.2.1.4	Konfigurasi System Logging.....	82
4.3.2.1.5	Konfigurasi Syslog Server The Dude .....	88
4.3.2.1.6	Konfigurasi Syslog Server Mikrotik Syslog.....	95
4.3.2.1.7	Konfigurasi System Script.....	98
4.3.2.1.8	Konfigurasi Tool Schdule.....	104
4.3.2.1.9	Konfigurasi Firewall Rule .....	106
4.3.2.2	Konfigurasi Reactive IDS .....	112
4.3.2.2.1	Konfigurasi Terhadap FTP Bruteforce .....	113
4.3.2.2.2	Konfigurasi Terhadap SSH Bruteforce.....	122
4.3.2.2.3	Konfigurasi Terhadap ICMP Flood .....	128
4.4	Pembahasan Sistem .....	135
4.4.1	Pengujian Reactive IDS .....	135
4.4.1.1	Fungsionalitas Test .....	137
4.4.1.1.1	Serangan FTP Bruteforce.....	138
4.4.1.1.2	Serangan SSH Bruteforce .....	145
4.4.1.1.3	Serangan ICMP Flood .....	151
4.4.1.2	Respon Time Test .....	158
4.4.1.2.1	Respon Time Serangan FTP Bruteforce .....	159
4.4.1.2.1.1	Serangan Berurutan .....	159
4.4.1.2.1.2	Serangan Bersamaan .....	160
4.4.1.2.2	Respon Time Serangan SSH Bruteforce.....	161



4.4.1.2.2.1	Serangan Berurutan .....	161
4.4.1.2.2.2	Serangan Bersamaan .....	161
4.4.1.2.3	Responstime Serangan ICMP Flood .....	162
4.4.1.2.3.1	Serangan Berurutan .....	162
4.4.1.2.3.2	Serangan Bersamaan .....	163
4.4.1.2.4	Menurunkan Interval Penjadwalan .....	164
4.4.1.3	False Negative Dan Positive Test.....	166
4.4.1.3.1	False Negative Dan Positive Serangan FTP Bruteforce .....	167
4.4.1.3.2	False Negative Dan Positive Serangan SSH Bruteforce.....	167
4.4.1.3.3	False Negative Dan Positive ICMP Flood.....	168
4.5	Identifikasi.....	169
4.5.1	Masalah Teknis .....	169
4.5.2	Masalah Non Teknis .....	175
4.6	Pemeliharaan Sistem .....	176
4.7	Evaluasi Sistem .....	176
<b>BAB V</b>	.....	182
5.1	Kesimpulan.....	182
5.2	Saran.....	184
<b>DAFTAR PUSTAKA</b>	.....	185
<b>LAMPIRAN</b>	.....	187

## DAFTAR TABEL

Tabel 1.1 Rencana Kegiatan .....	10
Tabel 2.1 IP Address Classfull.....	26
Tabel 3.1 Kebutuhan Hardware Mikrotik .....	52
Tabel 3.2 Kebutuhan Hardware Syslog Server .....	53
Tabel 3.3 Daftar Biaya Hardware .....	55
Tabel 3.4 Daftar Biaya Software.....	56
Tabel 3.5 Daftar Biaya Software Pendukung.....	57
Tabel 4.1 Respon Time Serangan Berurutan FTP Bruteforce .....	159
Tabel 4.2 Respon Time Serangan Bersamaan FTP Bruteforce.....	160
Tabel 4.3 Respon Time Serangan Berurutan SSH Bruteforce.....	161
Tabel 4.4 Respon Time Serangan Bersamaan SSH Bruteforce .....	162
Tabel 4.5 Respon Time Serangan Berurutan ICMP Flood .....	163
Tabel 4.6 Respon Time Serangan Bersamaan ICMP Flood .....	164
Tabel 4.7 Respon Time Serangan Berurutan Dengan Menurunkan Interval Penjadwalan Script .....	165
Tabel 4.8 Respon Time Serangan Bersamaan Dengan Menurunkan Interval Penjadwalan Script .....	165
Tabel 4.9 False Negative Dan Positive Serangan FTP Bruteforce .....	167
Tabel 4.10 False Negative Dan Positive Serangan SSH Bruteforce .....	168
Tabel 4.11 False Negative Dan Positive Serangan ICMP Flood .....	168
Tabel 4.12 Peningkatan False Negative .....	171
Tabel 4.13 Pengujian Peningkatan Respon Time .....	175
Tabel 4.14 Pengujian Kakuratan Peningkatan Respon Time.....	175
Tabel 4.15 Evaluasi Instalasi Dan Konfigurasi.....	176
Tabel 4.16 Evaluasi Pengujian Sistem.....	179

## DAFTAR GAMBAR

Gambar 2.1 Jenis-jenis Jaringan .....	15
Gambar 2.2 Topologi Star.....	16
Gambar 2.3 Topologi Bus .....	17
Gambar 2.4 Topologi Ring .....	17
Gambar 2.5 Topologi Tree.....	18
Gambar 2.6 Topologi Mesh .....	19
Gambar 2.7 Topologi Hybrid.....	19
Gambar 2.8 OSI Layer .....	24
Gambar 2.9 Model DOD.....	26
Gambar 2.10 Atribut Keamanan Informasi.....	29
Gambar 2.11 Interupsi.....	30
Gambar 2.12 Intersepsi .....	31
Gambar 2.13 Modifikasi .....	31
Gambar 2.14 Fabrikasi.....	32
Gambar 2.15 IDS Terpusat .....	38
Gambar 2.16 IDS Distribusi Parsial.....	39
Gambar 2.17 IDS Terdistribusi Total .....	39
Gambar 2.18 Logo Mikrotik .....	40
Gambar 2.19 Firewall.....	43
Gambar 3.1 Logo Perusahaan .....	44
Gambar 3.2 Struktur Organisasi PT. Wahana Lintas Nusa Persada .....	46
Gambar 3.3 Topologi Saat Ini.....	48

Gambar 3.4 PC Router Mikrotik.....	53
Gambar 3.5 Syslog Server.....	54
Gambar 3.6 Gambaran Umum Sistem .....	60
Gambar 3.7 Alur Kerja Reactive IDS .....	61
Gambar 3.8 Topologi Implementasi Ractive IDS.....	63
Gambar 3.9 Proses Pendeteksian Serangan .....	64
Gambar 3.10 Proses Keseluruhan Sistem .....	66
Gambar 3.11 Prosedur Penjadwalan .....	67
Gambar 4.1 Implementasi Topologi Sistem .....	70
Gambar 4.2 Tampilan Awal Mikrotik.....	72
Gambar 4.3 Tampilan The Dude Versi 4.....	73
Gambar 4.4 Tampilan Mikrotik Syslog .....	74
Gambar 4.5 Tampilan Winbox.....	75
Gambar 4.6 Konfigurasi System Identity .....	77
Gambar 4.7 Konfigurasi NTP Client .....	78
Gambar 4.8 Konfigurasi Tool Email.....	80
Gambar 4.9 Uji Coba Pengiriman Pesan Email.....	82
Gambar 4.10 Konfigurasi System Logging .....	83
Gambar 4.11 Logging Local .....	85
Gambar 4.12 Konfigurasi Logging Remote.....	86
Gambar 4.13 Konfigurasi Add Rule Log.....	87
Gambar 4.14 Login The Dude .....	88
Gambar 4.15 The Dude Server Configuration.....	89

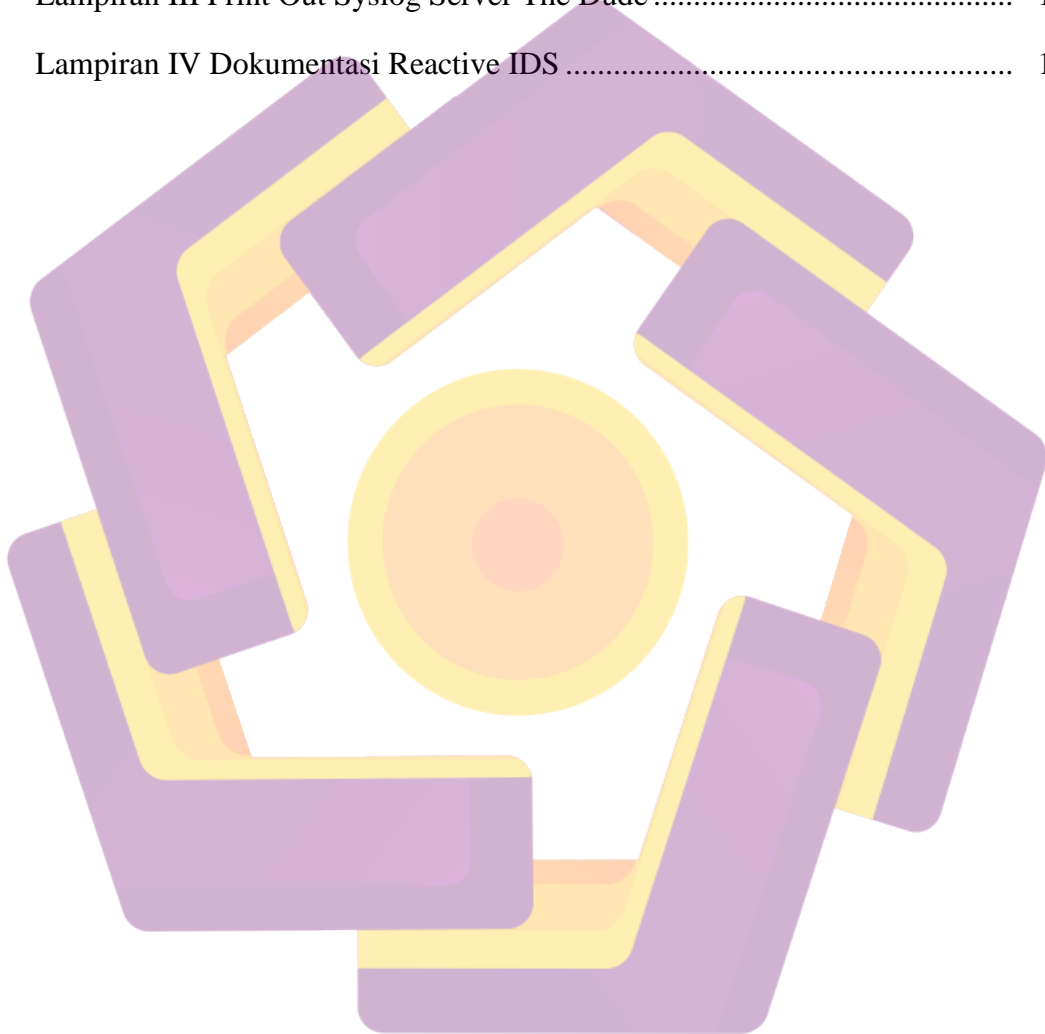
Gambar 4.16 The Dude Syslog Rule.....	90
Gambar 4.17 The Dude Add New Notification .....	91
Gambar 4.18 The Dude Sound Modification.....	93
Gambar 4.19 The Dude Log To Syslog .....	94
Gambar 4.20 The Dude Log Color Modification.....	94
Gambar 4.21 The Dude Syslog .....	95
Gambar 4.22 Mikrotik Syslog Option.....	96
Gambar 4.23 Mikrotik Syslog Configuration .....	97
Gambar 4.24 Mikrotik Syslog.....	97
Gambar 4.25 Script Repository.....	101
Gambar 4.26 Log Router.....	102
Gambar 4.27 Log Syslog Server The Dude.....	102
Gambar 4.28 Log Syslog Server Mikrotik Syslog .....	102
Gambar 4.29 Uji Coba Pengiriman Email .....	103
Gambar 4.30 Tool Schdule .....	105
Gambar 4.31 Hasil Log Schdule .....	106
Gambar 4.32 Uji Coba Firewall Filtering Rule.....	106
Gambar 4.33 Firewall Filter Rule .....	110
Gambar 4.34 Ping Sukses .....	110
Gambar 4.35 Ping Gagal.....	111
Gambar 4.36 Firewall Filter Address-list .....	112
Gambar 4.37 FTP Login Incorrect.....	114
Gambar 4.38 Skenario Serangan.....	136

Gambar 4.39 Tampilan Aplikasi BrutusA2 .....	139
Gambar 4.40 Uji Coba Serangan FTP Bruteforce .....	139
Gambar 4.41 Log FTP Bruteforce Pada Router .....	140
Gambar 4.42 Serangan FTP Bruteforce Gagal .....	141
Gambar 4.43 Pesan Error FTP Bruteforce .....	141
Gambar 4.44 Email Report FTP Bruteforce .....	142
Gambar 4.45 The Dude Syslog Server Serangan FTP Bruteforce.....	142
Gambar 4.46 Mikrotik Syslog Serangan FTP Bruteforce.....	143
Gambar 4.47 Address List FTP Bruteforce .....	144
Gambar 4.48 Laporan Mingguan FTP Bruteforce .....	144
Gambar 4.49 Notifikasi Pengiriman Laporan Mingguan.....	145
Gambar 4.50 Tampilan Aplikasi Putty.....	145
Gambar 4.51 SSH Bruteforce Berhasil .....	146
Gambar 4.52 Log SSH Bruteforce Pada Router .....	147
Gambar 4.53 SSH Bruteforce Gagal.....	147
Gambar 4.54 The Dude Serangan SSH Bruteforce.....	148
Gambar 4.55 Mikrotik Syslog Serangan SSH Bruteforce .....	148
Gambar 4.56 Email Report Serangan SSH Bruteforce .....	149
Gambar 4.57 Address List SSH Bruteforce .....	149
Gambar 4.58 Laporan Mingguan SSH Bruteforce.....	150
Gambar 4.59 Lampiran Laporan Mingguan SSH Bruteforce .....	150
Gambar 4.60 Notifikasi Pengiriman Laporan Mingguan.....	151
Gambar 4.61 Serangan ICMP Flood.....	152

Gambar 4.62 ICMP Flood Buffer Size 65000 .....	152
Gambar 4.63 Statistik ICMP Flood Buffer Size 65000 .....	153
Gambar 4.64 ICMP Flood Gagal .....	153
Gambar 4.65 Perintah Ping Yang Diizinkan.....	154
Gambar 4.66 Total Size Ping 32 Byte.....	154
Gambar 4.67 The Dude Serangan ICMP Flood.....	155
Gambar 4.68 Mikrotik Syslog Serangan ICMP Flood.....	155
Gambar 4.69 Email Report Serangan ICMP Flood .....	156
Gambar 4.70 Laporan Mingguan ICMP Flood.....	156
Gambar 4.71 Lampiran Laporan Mingguan ICMP Flood .....	157
Gambar 4.72 Notifikasi Pengiriman Laporan Mingguan.....	157
Gambar 4.73 Address List ICMP Flood .....	158
Gambar 4.74 Ilustrasi Penjadwalan Respon (Script) .....	170
Gambar 4.75 Ilustrasi Penjadwalan Report Tiga Serangan .....	170
Gambar 4.76 Ilustrasi Peningkatan False Negative .....	172

## DAFTAR LAMPIRAN

Lampiran I Surat Ijin Penelitian.....	188
Lampiran II Hasil Wawancara Dan Observasi.....	189
Lampiran III Print Out Syslog Server The Dude .....	192
Lampiran IV Dokumentasi Reactive IDS .....	194





## INTISARI

PT. Wahana Lintas Persada yang merupakan salah satu *Internet Service Provider* (ISP) menyadari bahwa semakin bertambahnya pelanggan, semakin meningkatnya node pada jaringan wahana yang harus selalu dimonitoring guna meningkatkan layanan *technical support* yang selalu *stanby* 24 jam. Kebutuhan akan sistem keamanan jaringan menjadi salah satu aspek yang perlu diperhatikan untuk meningkatkan layanan kepada pelanggan.

Membangun sistem peringatan dini atau IDS (*Intrusion Detection System*) merupakan salah satu solusi pemecahan masalah tersebut. Sistem ini bekerja dengan cara mendeteksi adanya serangan dan memberikan peringatan (*alert*) kepada administrator jaringan apabila terjadi serangan pada jaringan, selain itu IDS juga dapat digunakan untuk melakukan monitoring jaringan. Reactive IDS adalah IDS yang dapat melakukan *auto respon* berupa tindakan pencegahan saat terjadi serangan dan menampilkan peringatan serta mengirim *report* email.

Sistem Reactive IDS ini menggunakan mikrotikOS dan tool winbox dan beberapa tools untuk melakukan percobaan penyerangan terhadap jaringan. Pengujian sistem ini dilakukan dengan menggunakan beberapa jenis serangan ke jaringan dan pengujian fungsionalitas sistem adalah dengan melakukan cek peringatan (*alert*) dan report berupa email yang berisi IP penyerang untuk dikirim ke email administrator, guna membantu administrator *mobile* dalam melakukan monitoring jaringan.

**Kata Kunci** : Reactive IDS, winbox, ftp bruteforce, ICMP Flood, SSH bruteforce.

## **ABSTRACT**

*PT. Wahana Lintas Nusa Persada which is one of the Internet Service Providers (ISPs) realize that the increasing customers, increasing network node on a vehicle that should always be monitored in order to improve technical support services are always standby 24 hours. The need for network security systems into one of the aspects that need to be considered to improve the service to customers.*

*Build an early warning system or IDS (Intrusion Detection System) is one of the problem-solving solutions. This system works by detecting the presence of attacks and provides a warning (alert) to the network administrator in case of an attack on the network, in addition to the IDS can also be used to perform network monitoring. IDS is a reactive IDS can perform auto response form precautions during the attack and displays a warning and sends an email report.*

*Reactive IDS system uses mikrotikOS and Winbox tool and some tools to conduct attacks against the network experiments. System test is performed using several types of attacks to the network and testing the functionality of the system is to do a check warning (alert) and a report in the form of an email containing the attacker's IP to be sent to the email administrator, to assist administrators in monitoring mobile networks.*

**Keywords:** *Reactive IDS, Winbox, ftp bruteforce, ICMP Flood, SSH bruteforce.*