

**RANCANG BANGUN SISTEM KEAMANAN JARINGAN KOMPUTER
BERBASIS SNORT- INTRUSION DETECTION SYSTEM (IDS) DAN
WEB MONITORING PADA PT.BANGKA BINTANG LESTARI
PANGKALPINANG**

SKRIPSI



Dian Nugeraha Putra
0911500100

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG
2014**

**RANCANG BANGUN SISTEM KEAMANAN JARINGAN KOMPUTER
BERBASIS SNORT- INTRUSION DETECTION SYSTEM (IDS) DAN
WEB MONITORING PADA PT.BANGKA BINTANG LESTARI
PANGKALPINANG**

SKRIPSI

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**



oleh:
Dian Nugeraha Putra
0911500100

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG
2014**



LEMBAR PERNYATAAN

Yang bertandatangan di bawah ini :

NIM : 0911500100

Nama : Dian Nugeraha Putra

JudulSkripsi : **RANCANG BANGUN SISTEM KEAMANAN JARINGAN
KOMPUTER BERBASIS SNORT- INTRUSION
DETECTION SYSTEM (IDS) DAN WEB MONITORING
PADA PT.BANGKA BINTANG LESTARI
PANGKALPINANG**

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 14 Agustus 2014



(Dian Nugeraha Putra)

LEMBAR PENGESAHAN SKRIPSI

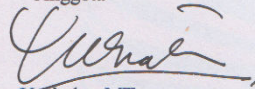
**RANCANG BANGUN SISTEM KEAMANAN JARINGAN KOMPUTER
BERBASIS SNORT- INTRUSION DETECTION SYSTEM DAN WEB
MONITORING PADA PT.BANGKA BINTANG LESTARI
PANGKALPINANG**

Yang dipersiapkan dan disusun oleh

Dian Nugeraha Putra
0911500100

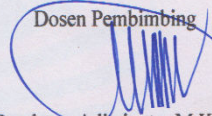
Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 21 Agustus 2014

Anggota



Yurindra, MT
NIDN. 0429057402

Dosen Pembimbing



Bambang Adiwinoto, M.Kom
NIDN. 0216107102

Ketua



Ellya Helmud, M.Kom
NIDN. 0201027901

Kaprodi Teknik Informatika




Sujono, M.Kom
NIDN. 0211037702

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Agustus 2014

KETUA STMIK ATMA LUHUR PANGKALPINANG




Dr. Saedjono, M.Sc

KATA PENGANTAR

Alhamdulillah, segala puja dan puji syukur saya panjatkan kehadirat Allah SWT, atas segala rahmat dan hidayahnya, shalawat serta salam kepadaNya sehingga saya dapat menyelesaikan skripsi ini sesuai dengan apa yang saya harapkan. skripsi ini disusun sebagai suatu syarat untuk mencapai tahap kelulusan dalam proses perkuliahan, mudah-mudahan menjadi karya yang spektakuler. Skripsi ini disusun untuk memenuhi sebagian syarat yang ditetapkan dalam rangka mengakhiri studi pada jenjang Strata Satu (S1) Teknik Informatika di STMIK ATMA LUHUR Pangkal Pinang. Dengan selesainya penyusunan skripsi ini, saya tidak lupa menyampaikan terima kasih yang sebesar-besarnya kepada pihak-pihak yang telah mendukung dalam penyusunan skripsi saya ini, antara lain kepada :

1. Bapak dan Ibu tercinta yang tidak akan pernah lelah mendukung serta memberikan semangat lahir dan batin bagi penulis.
2. Bapak Drs. DjaetunHs yang telah mendirikan STMIK Atma Luhur.
3. Bapak Dr. Moedjiono, Msc, selaku ketua STMIK Atma Luhur.
4. BapakSujiono, M.Kom selaku Kaprodi Teknik Informatika.
5. Bapak Bambang Adiwino, M.Kom selaku dosen pembimbing.
6. Bapak Ind ra Gunawan Selaku Pimpinan di Perusahaan PT.Bangka Bintang Lestari Pangkalpinang yang telah member izin untuk penulis melakukan riset.
7. Bapak Muhamad Uta, SH selaku HRD di Perusahaan PT.Bangka Bintang Lestari Pangkal Pinang yang telah memberikan bimbingan maupun materi selama penulis melakukan Riset.

Saya menyadari sekali bahwa dalam penulisan skripsi ini masih jauh dari kesempurnaan. Dengan segala kerendahan hati saya mohon maaf dan berharap skripsi ini dapat berguna dan bermanfaat bagi semua. Dan saya berharap skripsi yang saya susun ini menjadi suatu karya yang baik serta menjadi suatu persembahan terbaik bagi para dosen-dosen dan teman-teman yang berada di STMIK Atma Luhur dan Perusahaan PT.Bangka Bintang Lestari. Demikianlah kata pengantar dari saya dan sebagai suatu introspeksi diri, saya mohon maaf atas kekurangan dan kesalahannya. Dan kekurangan hanya terdapat pada diri saya, karena kebenaran sejati hanya milik Allah SWT saya ucapkan terima kasih.

Pangkalpinang, Agustus 2014

(Dian Nugeraha Putra)

ABSTRAKSI

Pada saat ini beberapa komputer yang ada di PT.Bangka Bintang Lestari sama sekali belum mempunyai sebuah jaringan yang dapat saling terkoneksi antar satu dengan yang lain sehingga proses komunikasi data antar satu unit bagian dengan yang lain masih sering mengalami suatu keterlambatan baik di dalam perusahaan maupun ke pusat, sehingga untuk mengatasi masalah ini diusulkan lah untuk membuat sebuah jaringan komputer di dalam ruang lingkup perusahaan.

Terlepas dari permasalahan tersebut pihak dari manajemen perusahaan berfikir jika di dalam sebuah perusahaan jika terdapat sebuah jaringan komputer tentu saja akan sangat rentan terhadap aktivitas kejahatan baik dari dalam ataupun luar perusahaan yang mencoba mencari informasi penting dari perusahaan, hal ini tentu saja dapat berdampak buruk bagi perusahaan, tentu saja sebuah perusahaan harus mempunyai sistem keamanan yang cocok di dalam jaringannya,

Oleh karena itu penulis mempunyai pikiran untuk mengusulkan kembali membangun sebuah sistem keamanan dan jaringan komputer pada perusahaan PT.BANGKA BINTANG LESTARI yang berbasis *Intrusion Detection System (IDS)* yang *Open Source* dengan menggunakan snort,Barnyard,BASE web monitoring lengkap dengan tampilan grafis dengan beberapa fitur tambahan beserta penggunaan *iptables Firewall* sehingga dapat mempermudah *administrator* dalam memonitor kondisi jaringannya dari para intruder dari luar maupun dalam yang mencoba masuk mencari informasi. dan dapat membantu perusahaan itu sendiri dalam berkomunikasi data dengan baik dan bisa menjadi sebuah referensi bagi perusahaan untuk tahap pengembangan selanjutnya

Kata Kunci : *Intrusion Detection System, Snort, BASE, iptables, Firewall*

DAFTAR ISI

LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN SKRIPSI	ii
KATA PENGANTAR.....	iii
ABSTRAKSI.....	iv
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xiv
BAB I PENDAHULUAN	
1.1 LatarBelakang.....	1
1.2 RumusanMasalah.....	4
1.3 BatasanMasalah	4
1.4 TujuanPenelitian	5
1.5 MetodePenelitian	5
a. Studi literatur dan pustaka	5
b. Studi Lapangan.....	6
c. Analisa dan perancangan system.....	6
1) Tahap Analisa.....	6
2) Tahap Perancangan	6
d. Implementasi perancangan perangkat lunak.....	6
1) Tahap Implementasi.....	6
e. Uji Coba Dan Evaluasi Sistem.....	6
f. Mengambil Kesimpulan.....	7
1.6 SistematikaPenulisan	7
BAB II LANDASAN TEORI	
2.1 Pengertian Rancang Bangun.....	9
2.2 Definisi Sistem Keamanan	9
2.3 Jaringan Kompter.....	9
2.3.1. Konsep Dan Arsitektur Jaringan.....	9

2.3.1.1. Klasifikasi Jaringan	10
2.3.1.2. Berdasarkan Media Tranmisi	11
2.3.1.3. Berdasarkan Fungsi	12
2.3.2. Pengertian Topologi Jaringan	13
2.3.3. Komponen Perangkat Jaringan	16
2.3.4. Protokol Jaringan.....	20
2.3.5. Model OSI (<i>Open System Interconetion</i>)	20
2.3.6. Model TCP/IP	22
2.3.7. IP Address (<i>Internet Protocol Address</i>)	23
2.3.8. Subnet Mask Dan Subnetting.....	24
2.3.9. Bandwith.....	27
2.3.10. Mac Address	27
2.3.11. DNS (<i>Domain Name System</i>).....	28
2.3.12. DHCP (<i>Dyanmic Host Configuration Protocol</i>).....	28
2.3.13. <i>Internet Service Provider</i> (ISP).....	28
2.3.14. Gateway	29
2.4. Jaringan Wireless.....	29
2.4.1. Definisi dan Konsep Jaringan Wireless.....	29
2.4.2. Teknologi Jaringan Wireless	30
2.4.3. Topologi Jaringan Wireless	31
2.4.4. SSID (<i>Service Set Indetifier</i>).....	32
2.4.5. Kelebihan Dan Kelemahan Jaringan Wireless.....	32
2.5. Keamanan Jaringan.....	33
2.5.1. Konsep Keamanan Jaringan.....	33
2.5.2. Tujuan Keamanan Jaringan	34
2.5.3. Access Control.....	35
2.5.4. Kebijakan Keamanan	35
2.6. Pengertian Hacker Dan Cracker	38
2.6.1. Hirarki Tingkatan Hacker.....	39
2.6.2. Langkah-langkah Hacker Menembus Sistem	41
2.7. Jenis-Jenis Serangan	45

2.8. Firewall	48
2.7.1. Definisi dan Konsep Firewall	48
2.7.2. Karakteristik Firewall	49
2.7.3. Teknik Pengamanan Firewall	49
2.7.4. Jenis-jenis Firewall.....	49
2.7.5. Konfigurasi Firewall.....	50
2.8. Intrusion Detection System (IDS)	51
2.8.1. Definisi Dan Konsep IDS	51
2.8.2. Jenis Intrusion Detection System (IDS)	52
2.8.3. Intrusion Detection System Mengenal adanya Intruder	55
2.8.4. Melindungi IDS.....	56
2.8.5. Fungsi IDS (<i>Intrusion Detection System</i>).....	57
2.8.6. Peran IDS (<i>Intrusion Detection System</i>).....	58
2.8.7. Keuntungan Dan Kekurangan IDS.....	60
2.8.8. Prinsip Kerja IDS Pada Jaringan Internal.....	61
2.8.9. Tujuan Penggunaan IDS	63
2.9. Perangkat Lunak Dan Perangkat Keras.....	64
2.9.1. Snort	64
2.9.1.1. Definisi Dan Konsep Snort.....	64
2.9.1.2. Fitur–Fitur Snort.....	65
2.9.1.3. Komponen-Komponen Snort.....	66
2.9.1.4. Snort.conf File.....	68
2.9.1.5. Proses Pendeteksian Pada Snort.....	68
2.9.1.6. Penempatan Intrusion Detection System	69
2.9.1.7. Penempatan Sensor.....	70
2.9.1.8. Klasifikasi Serangan.....	71
2.9.1.9. IDS Support Platform.....	73
2.9.1.10. Program Dan Produk IDS	74
2.10. IP TABLES.....	75
2.11. BASE (Basic Analysis Security Engine).....	75
2.12. Digital Blaster	75

2.13. Nmap	76
2.14. Wireshark	76
BAB III PEMODELAN PROYEK	
3.1. Definisi Proyek	77
3.2. Objective Proyek.....	77
3.3. Identifikasi Stakeholder	80
3.4. Identifikasi Deliveriabies	81
3.5. Penjadwalan Proyek.....	82
3.5.1 Ekstimasi Waktu Pelaksanaan.....	83
3.5.2 Work Breakdown Struktur	87
3.5.3 Milistone.....	88
3.5.4 Jadwal Proyek.....	89
3.6. Rencana Anggaran Biaya (RAB).....	91
3.7. Tim Proyek	93
3.8. Analisa Resiko.....	94
3.9. Meeting Plan.....	95
BAB IV ANALISA DAN PERANCANGAN	
4.1. Sejarah Singkat PT.Bangka Bintang Lestari	96
a. Filosofi Organanisasi.....	96
b. Visi Organisasi	96
c. Misi Organisasi	97
4.1.1. Struktur Organisasi.....	97
4.1.2. Tugas Pokok Dan Fungsi.....	98
4.2. Aktivitas Perusahaan (Rich Picture)	101
4.3. Analisa Fisik Struktur Komputer.....	103
4.3.1. Analisa Fungsi Bagian/unit.....	104
4.3.2. Analisa Pengguna.....	104
4.3.3. Analisa Perangkat Keras.....	105
4.3.4. Analisa Perangkat Lunak.....	106
4.4. Perancangan (Design)	107
4.4.1. Perancangan Jaringan Komputer.....	107

4.4.2. Perancangan Topologi Jaringan.....	108
4.4.3. Perancangan Topologi Sistem.....	108
4.4.4. Perancangan Sistem Keamanan IDS	111

BAB V IMPLEMENTASI DAN PEMBAHASAN

5.1. IMPLEMENTASI.....	114
5.2. Implementasi Topologi Jaringan	114
5.3. Implementasi Dan Konfigurasi IDS.....	114
5.3.1. Instalasi Paket Dependency	115
5.3.2. Instalasi Paket Snort	122
5.3.3. Instalasi Rules Snort.....	125
5.3.4. Konfigurasi File Snort.Conf	127
5.3.5. Setup Database Snort.....	130
5.3.6. Konfigurasi Barnyard	134
5.3.7. Konfigurasi Barnyard2.conf	135
5.3.8. Konfigurasi Adodb	137
5.3.9. Konfigurasi BASE.....	139
5.4. Pengoperasian Snort.....	152
5.4.1. Sniffer Mode	152
5.4.2. Packet Logger Mode	152
5.4.3. Intrusion Detection Mode	153
5.5. Monitoring.....	154
5.5.1. Pengujian Sistem IDS.....	155
5.5.2. Pengujian IDS Dengan TCP Flooding	155
5.5.3. Ping Attack (ICMP Traffic).....	159
5.5.4. Nmap PortScanning Attack	160
5.6. Analisa Data Menggunakan Base	163
5.7. Pencegahan Serangan Menggunakan IPTABLES	166
5.8. Keuntungan Dan Hasil Menggunakan IDS	175
5.9. Kesimpulan Dan Saran.....	176
DAFTAR PUSTAKA.....	178
LAMPIRAN.....	180

DAFTAR GAMBAR

Gambar 2.1.Topologi Bus	14
Gambar 2.2.Topologi Ring.....	14
Gambar 2.3.Topologi star	15
Gambar 2.4.Model OSI.....	21
Gambar 2.5.IP Address Reprntasi Dalam Biner	24
Gambar 2.6.Komponen Hubungan Snort.....	68
Gambar 2.7.Proses Pendeteksian Snort	69
Gambar 3.1.Work Breakdown Strukture (WBS)	84
Gambar 3.2.Milistone	85
Gambar 3.3.Jadwal Proyek.....	86
Gambar 3.4.Diagram Batang.....	87
Gambar 3.5.Struktur Tim Proyek	91
Gambar 4.1.Struktur Organisasi	97
Gambar 4.2.Rich Picture	100
Gambar 4.3.Struktur Komputer	102
Gambar 4.4.Perancangan Topologi Jaringan	107
Gambar 4.5.Toplogi Jaringan IDS.....	110
Gambar 4.6.Diagram Flowchart Perancangan Sistem IDS.....	112
Gambar 5.1.Proses Install Mysql-Common	114
Gambar 5.2.Proses Install Mysql-Client	115
Gambar 5.3.Proses Install Mysql-Server	115
Gambar 5.4.Installasi Php5-dev	116
Gambar 5.5.Installasi Php5-ldap	116
Gambar 5.6.Installasi php5-mysql.....	117
Gambar 5.7.Installasi Libcap.....	117
Gambar 5.8.Installasi Libpcrc3-dev	118
Gambar 5.9.Installasi Expect.....	118
Gambar 5.10.Installasi Bison	119

Gambar 5.11.Installasi Libmysql++dev.....	119
Gambar 5.12.Installasi Libapache2-mod-php5	120
Gambar 5.13.Installasi php5-cgi.....	120
Gambar 5.14.Ekstrak Snort	122
Gambar 5.15.Proses Konfigurasi Mysql.....	122
Gambar 5.16.Prose Make File Snort	123
Gambar 5.17.Proses Make Install Snort	123
Gambar 5.18.Membuat Direktori Snort	124
Gambar 5.19.Proses Ekstrak Rules Snort	125
Gambar 5.20.Proses Compile Paket Rule Snort.....	125
Gambar 5.21.Tampilan Awal File Snort.conf	126
Gambar 5.22.Lokasi Signature Rules Snort.....	127
Gambar 5.23.Set Output Database Snort	127
Gambar 5.24.Set Format Binary Alert Dan Logging Snort	128
Gambar 5.25.Uji Coba Snort.....	128
Gambar 5.26.Hasil Uji Coba Snort.....	129
Gambar 5.27.Proses Pembuatan Database Snort.....	130
Gambar 5.28.Proses Penyiapan Database Snort.....	131
Gambar 5.29.Login Ke Database Snort	132
Gambar 5.30.Menampilkan Database Snort	132
Gambar 5.31.Menampilkan Table Database	133
Gambar 5.32.Pengcopyan Folder Adodb.....	135
Gambar 5.33.Proses Masuk Direktori Lain.....	135
Gambar 5.34.Proses Compile File Adodb	136
Gambar 5.35.Installasi Paket php-pear Base.....	137
Gambar 5.36.Installasi Modul Pear	137
Gambar 5.37.Installasi Paket Number_Roman php	138
Gambar 5.38.Installasi Paket Number_Words php	138
Gambar 5.39.Installasi Paket Image_Canvas php	139
Gambar 5.40.Installasi Paket Image_Graph php.....	139
Gambar 5.41.Installasi Paket Alldeps_Mail php.....	140

Gambar 5.42.Installasi Paket Mail_Mime	140
Gambar 5.43.Pengcopyan Folder Base	141
Gambar 5.44.Proses Compile File Base	142
Gambar 5.45.Mengganti Folder Base	142
Gambar 5.46.Masuk Ke Direktori Base.....	143
Gambar 5.47.Copy File Base_conf.php.dist	143
Gambar 5.48.Edit Konfigurasi Lokasi	144
Gambar 5.49.Edit Lokasi Path Database	145
Gambar 5.50.Edit Konfigurasi Database	145
Gambar 5.51.Perintah Untuk Apache Web Server mengakses BASE	146
Gambar 5.52.Restart Apache Dan Mysql	146
Gambar 5.53.Tampilan Browser Base Setup 1	147
Gambar 5.54.Tampilan Browser Base Setup 2	147
Gambar 5.55.Tampilan Browser Base Setup 3	148
Gambar 5.56.Tampilan Browser Base Setup 4	148
Gambar 5.57.Tampilan Browser Base Setup 5	149
Gambar 5.58.Tampilan Browser Base Setup 6	149
Gambar 5.59.Tampilan Login Browser Base.....	150
Gambar 5.60.Tampilan Muka Browser Base	150
Gambar 5.61.Proses TCP Dan UDP Flood Ke Server Linux	154
Gambar 5.62.Scanning Port TCP Dan UDP Flood Ke Server Linux	155
Gambar 5.63.Perekaman Data Hasil Monitoring Wireshark	156
Gambar 5.64.Hasil Deteksi Snort IDS Dan Wireshark	156
Gambar 5.65.Hasil Deteksi IDS TCP Flooding	157
Gambar 5.66.Proses Ping Attack.....	159
Gambar 5.67.Hasil deteksi Snort IDS Ping Attack	159
Gambar 5.68.Proses Scanning Nmap Ke Server	160
Gambar 5.69.Hasil Info deteksi Nmap Ke Server	160
Gambar 5.70.Hasil Info Deteksi Port Yang Terbuka	161
Gambar 5.71.Hasil Deteksi Nmap Di IDS	161
Gambar 5.72.Hasil Deteksi IDS Scanning Port Nmap	162

Gambar 5.73.Halaman Utama Base.....	163
Gambar 5.74.Alert Yang Ditampilkan.....	164
Gambar 5.75.Tampilan Daftar Alert Dan Traffic.....	164
Gambar 5.76.Alert Time Yang Ditampilkan.....	165
Gambar 5.77.Blok Target Dengan IPTABLES.....	167
Gambar 5.78.Menampilkan Aturan IPTABLE Yang Dibuat.....	169
Gambar 5.79.Hasil Aturan Yang Telah Dibuat.....	170
Gambar 5.80.Proses Flooding Setelah Di REJECT	171
Gambar 5.81.Hasil DROP Ping Attack.....	172
Gambar 5.82.Hasil Scan Nmap Tidak Menampilkan Info Server.....	173
Gambar 5.83.Hasil Nmap Tidak Menampilkan Port yang Terbuka.....	174

DAFTAR TABEL

Tabel 2.1.IPV4.....	24
Tabel 2.2.Subnet Mask Defalult.....	25
Tabel 2.3.IP Privat.....	26
Tabel 2.4.Subnetting Kelas C.....	26
Tabel 2.5.Standart IEEE 802.11.....	30
Tabel 2.6.Jenis Serangan.....	48
Tabel 2.7.Perbandingan NIDS Dan HIDS.....	53
Tabel 2.8.Klasifikasi Serangan Berdasarkan Tingkat Priority.....	71
Tabel 3.1.Kegiatan Task.....	81
Tabel 3.2.Ekstimasi Waktu Pelaksanaan WBS.....	82
Tabel 3.3.Rencana Anggaran Biaya.....	88
Tabel 3.4.Meeting Plan.....	92
Tabel 4.1.Spesifikasi Perangkat Keras.....	104
Tabel 4.2.Spesifikasi PC Server (IDS).....	105
Tabel 4.3.Penambahan Perangkat Jaringan.....	106
Tabel 4.4.Rincian Topologi Fisik.....	108
Tabel 4.5.Rincian IP Topologi Fisik.....	109
Tabel 4.6.Komponen Mesin Sensor IDS.....	111