

**PERANCANGAN DAN IMPLEMENTASI DETEKSI INTRUSI DAN
SISTEM PENCEGAHAN (IDPS) DI SERVER CENTOS
Studi Kasus : Yogya Crew/Indonesian Backtrack Team reg. Yogyakarta**

SKRIPSI



disusun oleh

Mahmudi

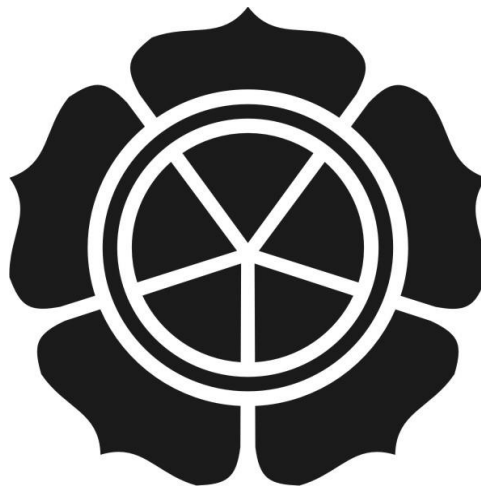
10.11.4343

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

**PERANCANGAN DAN IMPLEMENTASI DETEKSI INTRUSI DAN
SISTEM PENCEGAHAN (IDPS) DI SERVER CENTOS
Studi Kasus : Yogya Crew/Indonesian Backtrack Team reg. Yogyakarta**

SKRIPSI

Untuk memenuhi sebagai persyaratan
Mencapai derajat Sarjana S1
Pada jurusan Teknik Informatika



disusun oleh

Mahmudi

10.11.4343

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

PERSETUJUAN

SKRIPSI

**PERANCANGAN DAN IMPLEMENTASI DETEKSI INTRUSI DAN
SISTEM PENCEGAHAN (IDPS) DI SERVER CENTOS**

Studi Kasus : Yogya Crew/Indonesian Backtrack Team reg. Yogyakarta

yang disusun oleh:

Mahmudi

10.11.4343

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 23 Juni 2014
Dosen Pembimbing,



Kusnawi, S.Kom, M. Eng.
NIK. 190302112

PENGESAHAN

SKRIPSI

**PERANCANGAN DAN IMPLEMENTASI DETEKSI INTRUSI DAN
SISTEM PENCEGAHAN (IDPS) DI SERVER CENTOS**
Studi Kasus : Yogya Crew/Indonesian Backtrack Team reg. Yogyakarta

yang disusun oleh:

Mahmudi

10.11.4343

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 September 2014

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

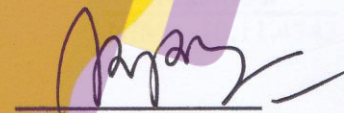
Kusnawi, S.Kom, M.Eng
NIK. 190302112



Akhmad Dahlan, M.Kom
NIK. 190302174



Krisnawati, S.Si, MT
NIK. 190302038



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



KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.

NIK. 190302001

PERNYATAAN

Saya yang bertandatangan di bawah 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, 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.

Yogyakarta, 29 September 2014

Mahmudi
NIM : 10.11.4343

PERSEMBAHAN

Seiring rasa syukurku karya ini kupersembahkan untuk :

- Kepada Allah SWT yang telah memberikan rahmat dan hidayahnya sehingga skripsi ini dapat terselesaikan dengan baik.
- Bapakku **Bungkari** dan Ibukku **Taslimah** tercinta yang telah mencurahkan segala kasih sayang dan jerih payah menuntunku agar menjadi yang terbaik dan senantiasa mengiringi setiap langkahku dengan doa dan ridhonya.
- Tak lupa kubingkiskan karya kecil ini untuk adikku **Isnaini Solichah** dan **Keluarga Besarku** yang telah memberikan doa dan dukungannya selama ini, terima kasih.
- Teman-temanku yang tidak bisa saya sebutkan satu per satu serta semua shabat-sahabatku yang selalu memotivasiku yang selalu ada setiap saat setiap waktu, terimakasih untuk semuanya.

MOTTO

“Sabar dalam mengatasi kesulitan dan bertindak bijaksana dalam mengatasinya
adalah sesuatu yang utama”

“Sehari menunda skripsi bearti sehari menunda kesuksesan”

“Belajar dan terus hargai proses”



KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa yang telah senantiasa mencurahkan berkat, anugerah, dan cinta kasih-Nya kepada setiap umat-Nya. Skripsi ini merupakan salah satu hasil dari karunia Allah dalam kehidupan penulis.

Skripsi ini disusun sebagai salah satu syarat kelulusan Program Strata 1 Jurusan Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer “AMIKOM” Yogyakarta dan untuk memperoleh gelar Sarjana Komputer.

Dengan selesainya Skripsi yang berjudul *Perancangan Dan Implementasi deteksi intrusi dan sistem pencegahan (IDPS) di Server CentOS (Studi kasus : Yogya Crew/Indonesian Backtrack Reg. Yogyakarta)*. Dengan ini penyusun mengucapkan banyak terima kasih kepada :

1. Bapak Prof. Dr. H.M Suyanto, MM. selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer “AMIKOM” Yogyakarta.
2. Drs. Sudarmawan, MT. Selaku Ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Kusnawi, S.KOM, M. ENG. selaku Dosen Pembimbing yang telah memberikan banyak masukan yang membantu dalam menyelesaikan skripsi ini.
4. Staf dan karyawan Sekolah Tinggi Manajemen Informatika dan Komputer “AMIKOM” Yogyakarta.
5. Yogya Crew/Indonesian Backtrack Team reg. Yogyakarta yang telah mengizinkan melakukan penelitian dan membantu selama proses penelitian.
6. Mas Ikbal a.k.a Ikon’s pirasi selaku sysadmin Tecon di olso.

7. Mas Suwandono a.k.a suro selaku pimpinan BLC Telkom klaten.
8. Teman - teman khususnya teman dekat.

Serta semua pihak yang telah membantu dalam penyelesaian skripsi ini yang tidak bisa saya sebutkan satu per satu. Selain itu penulis juga berterima kasih kepada semua peristiwa yang telah menambah semangat penulis dalam penulisan skripsi ini.

Akhir kata semoga skripsi ini dapat memberikan manfaat bagi pihak terkait, masyarakat umum dan khususnya bagi penyusun, skripsi ini masih terdapat kekurangan, oleh karena itu saran atau masukan dari pembaca sangat kami harapkan sebagai acuan untuk lebih baik di waktu yang akan datang.

Yogyakarta, 29 September 2014

Penulis

DAFTAR ISI

JUDUL	i
PERSETUJUAN	Error! Bookmark not defined.
PENGESAHAN	Error! Bookmark not defined.
PERNYATAAN	iv
PERSEMBAHAN	v
MOTTO	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xv
INTISARI	xviii
<i>ABSTRACT</i>	xix
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah	5
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	6
1.6 Metode Penelitian	6
1.7 Sistematika Penulisan	7
BAB II	10
LANDASAN TEORI	10

2.1	Definisi Perancangan.....	10
2.2	Pengertian Jaringan Komputer.....	11
2.2.1	Peer to peer.....	12
2.2.2	Client – Server.....	15
2.2.3	Kelebihan jaringan client server	17
2.2.3	Kekurangan jaringan client server	17
2.3	Sejarah Jaringan & Internet.....	18
2.4	Tujuan / Manfaat Jaringan Komputer	20
2.5	Manfaat jaringan komputer untuk umum:.....	21
2.6	Tentang keamanan Jaringan	22
2.6.1	Definisi Keamanan Jaringan	22
2.6.2	Prinsip keamanan jaringan	24
2.6.3	Ancaman keamanan jaringan	25
2.7	Deteksi intrusi dan sistem pencegahan (IDPS).....	32
2.7.1	Definisi Intrusi.....	32
2.7.2	Tentang Sistem IDPS	32
2.7.3	Fungsi Teknologi IDPS.....	35
2.7.4	Jenis Teknologi IDPS.....	39
2.7.5	Intrusion Detection System (IDS)	42
2.7.6	Intrusion Prevention System (IPS)	42
2.8	Software yang Digunakan.....	44
2.8.1	Linux CentOS	44
2.8.2	Snorby	44
2.8.3	Snort.....	45
2.8.4	Artillery.....	46

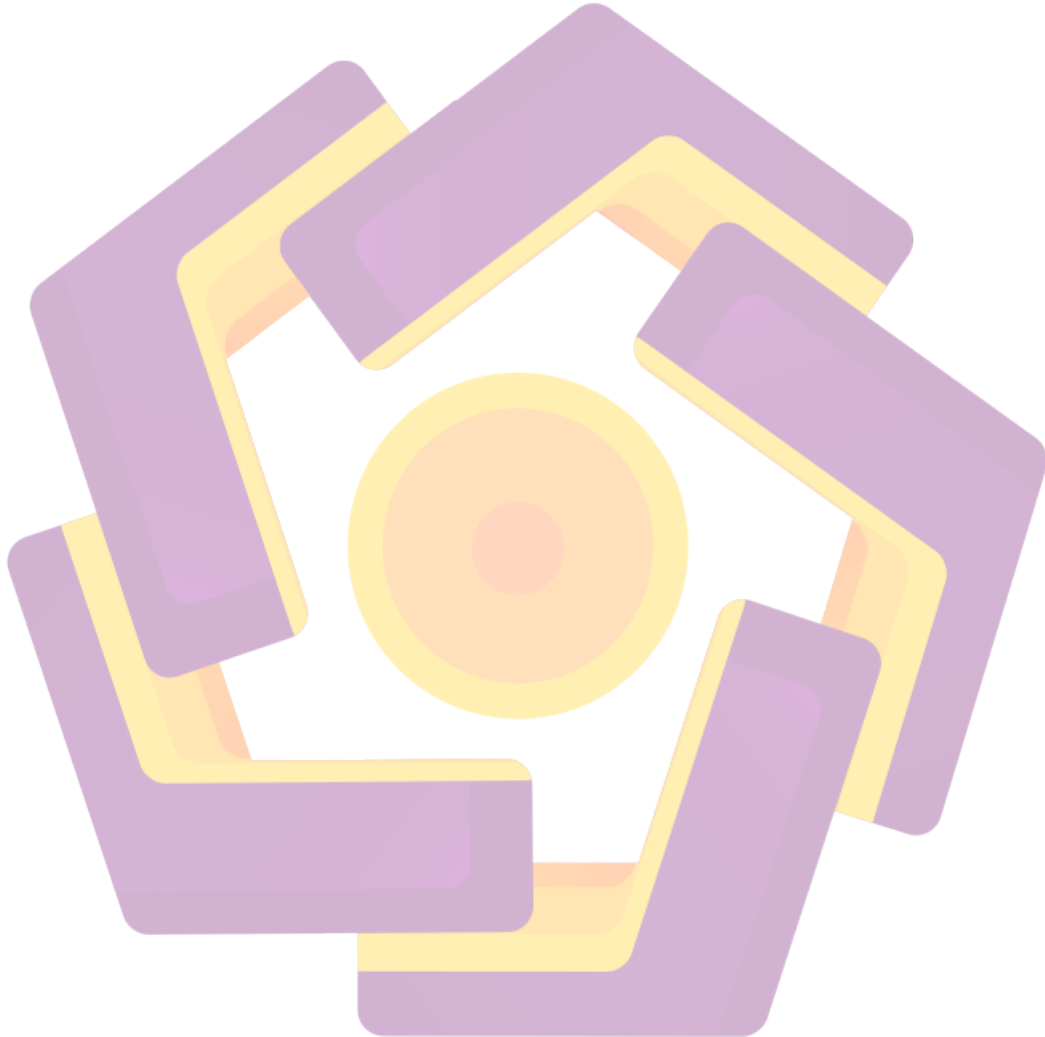
BAB III	49
ANALISIS DAN PERANCANGAN SISTEM	49
3.1 Yogya crew IT.....	49
3.1.1 Gambaran umum.....	49
3.1.2 Profile	49
3.1.3 Visi.....	50
3.1.4 Misi.....	50
3.1.5 Logo Yogyakarta IT	51
3.2 Analisis Sistem.....	51
3.2.1 Sistem Pendeteksi Jaringan	51
3.2.2 Laporan Analisa Jaringan	51
3.2.3 System Logging	52
3.2.4 Email Report Jaringan.....	52
3.2.5 Firewall.....	52
3.2.6 Topology Jaringan Saat Ini.....	53
3.3 Analisis SWOT	54
3.4 Analisa Kebutuhan System.....	55
3.4.1 Analisa Kebutuhan Fungsional	55
3.4.2 Analisa Kebutuhan Non Fungsional.....	55
3.4.3 Analisis Kelayakan Sistem	57
3.5 Perancangan Sistem.....	58
3.5.1 Gambaran umum.....	58
3.5.2 Topologi dan Sistem Kerja IDPS	59
3.5.3 Proses IDPS dalam membaca <i>network traffic</i> dan mengirimkan <i>log system</i> ke <i>sysadmin</i>	61

3.5.4	Proses IDPS dalam melakukan blocking dan melanjutkan <i>traffic</i> jaringan.....	61
BAB IV		63
IMPLEMENTASI DAN PEMBAHASAN.....		63
4.1	Instalasi Snort.....	63
4.1.1	Download snort.....	63
4.1.2	Ekstrak snort.....	63
4.1.3	Install snort	64
4.1.4	konfigurasi Snort startup.....	64
4.1.5	konfigurasi script start up snort.....	65
4.2	Install snort rules.....	67
4.2.1	Download snort rules.....	67
4.2.2	Ekstrak snort rules	68
4.2.3	Konfigurasi snort.conf.....	69
4.2.4	Tes konfigurasi snort.....	70
4.3	Install Barnyard2.....	71
4.3.1	Download Barnyard2	71
4.3.2	Genered paket barnyard2.....	72
4.3.3	Konfigurasi start up Barnyard2.....	72
4.3.4	Konfigurasi barnyard2 start up	73
4.4	Install Snorby	75
4.4.1	Install Snorby	75
4.4.2	Konfigurasi Snorby.....	75
4.4.3	Konfigurasi database snorby dan username dan password	76
4.4.4	Install Snorby	77

4.4.5	Konfigurasi output alert barnyard2 ke database snorby	78
4.4.6	Konfigurasi apache.....	79
4.4.7	Run snorby.....	81
4.5	Install Artillery	82
4.5.1	Download artillery	82
4.5.2	Install Artillery	83
4.5.3	Konfigursi Artillery	83
4.6	Ujicoba sistem deteksi dan pencegahan gangguan (IDPS)	85
4.6.1	Percobaan Informations Gathering.....	85
4.6.2	Percobaan Attack	88
4.7	Pembahasan sistem lama dengan sistem baru IDPS	89
4.7.1	Sistem Pendeteksi Jaringan	89
4.7.2	Laporan Analisa Jaringan	90
4.7.3	<i>System Logging</i>	92
4.7.4	Email Report Jaringan.....	93
4.7.5	<i>Firewall</i>	93
BAB V	95
PENUTUP	95
5.1	Kesimpulan.....	95
5.2	Saran	95
DAFTAR PUSTAKA	97

DAFTAR TABEL

Tabel 3.1 Analisis SWOT	54
Tabel 3.2 Spesifikasi Hardware Server	56



DAFTAR GAMBAR

Gambar 2.1 Peer to peer.....	13
Gambar 2.2 Client Server.....	14
Gambar 2.3 Model client server umum.....	16
Gambar 2.4 Model client server dengan dedicated server.....	17
Gambar 2.5 Jaringan komputer model TSS.....	19
Gambar 3.1 Logo yogyacrew IT.....	51
Gambar 3.2 Topologi jaringan lama.....	53
Gambar 3.3 Gambaran umum IDPS.....	59
Gambar 3.4 Topologi sistem baru.....	60
Gambar 3.5 Proses deteksi dan email log.....	61
Gambar 3.6 Proses bloking dan unbloking paket jaringan.....	62
Gambar 4.1 Download snort.....	63
Gambar 4.2 Ekstrak snort.....	64
Gambar 4.3 Install snort.....	64
Gambar 4.4 Snort startup.....	65
Gambar 4.5 Startup konfigurasi snort.....	65
Gambar 4.6 Edit snort startup.....	66
Gambar 4.7 Hapus code snort startup.....	66
Gambar 4.8 Edit sysconfig snort.....	66
Gambar 4.9 Sysconfig comment.....	67
Gambar 4.10 Download snortrules.....	68

Gambar 4.11 Ekstrak snortrules	69
Gambar 4.12 Edit snort.conf	69
Gambar 4.13 Tambahkan output.....	70
Gambar 4.14 Test snortrules	71
Gambar 4.15 Download barnyard2	72
Gambar 4.16 Ekstrak barnyard2	72
Gambar 4.17 Startup konfigurasi barnyard2.....	73
Gambar 4.18 Edit startup barnyard2	73
Gambar 4.19 Ganti angka menjadi 70	73
Gambar 4.20 Ganti L menjadi l	74
Gambar 4.21 Edit sysconfig barnyard2.....	74
Gambar 4.22 Edit log file.....	74
Gambar 4.23 Download snorby	75
Gambar 4.24 Snorby konfigurasi	76
Gambar 4.25 Edit database snorby	76
Gambar 4.26 Edit username dan password database	77
Gambar 4.27 Bundle install.....	77
Gambar 4.28 Jalankan snorby	78
Gambar 4.29 Edit barnyard2.conf	78
Gambar 4.30 Tambahkan output database snorby	79
Gambar 4.31 Edit apache snorby	79
Gambar 4.32 Tambahkan patch snorby di apache	80
Gambar 4.33 Tampilan login snorby	81

Gambar 4.34 Dashboard snorby.....	82
Gambar 4.35 Download artillery	82
Gambar 4.36 Install Artillery	83
Gambar 4.37 Ketik y dan enter	83
Gambar 4.38 Start artillery.....	83
Gambar 4.39 Monitoring direktori.....	84
Gambar 4.40 Port proteksi	85
Gambar 4.41 Dashboard awal ICMP	86
Gambar 4.42 Dashboard respon ICMP	86
Gambar 4.43 Dashboard awal NMAP	87
Gambar 4.44 Dashboard respon NMAP	87
Gambar 4.45 Dashboard respon LOIC	89
Gambar 4.46 Sensor IDS snort.....	90
Gambar 4.47 Signatures snortrules	90
Gambar 4.48 Eksport to PDF	91
Gambar 4.49 PDF log snorby.....	92
Gambar 4.50 GUI log snorby.....	93
Gambar 4.51 Banned list.....	94

INTISARI

Dalam perkembangan teknologi informasi saat ini pertukaran data dan informasi yang cepat sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan internet. Keamanan jaringan sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin keaslian data. Namun keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar. Berbagai macam ancaman dalam jaringan mulai hanya sekedar melakukan tes terhadap jaringan tersebut seperti *scanning* atau pun membuat jaringan menjadi lumpuh dengan melancarkan *Denial of Service (DoS)*, sampai usaha untuk mendapatkan informasi penting dari server.

Administrator bertanggung jawab penuh atas keamanan jaringan tersebut. Pengawasan harus dilakukan secara terus menerus untuk menjaga kualitas jaringan, karena kesalahan pada jaringan tidak bisa dideteksi kapan terjadinya. Hal ini berakibat buruk jika terjadi kesalahan jaringan yang tidak diketahui karena administrator jaringan sedang tidak ada di tempat pengawasan. Salah satu metode untuk mengawasi keamanan jaringan dengan menerapkan sistem IDPS (*Intrusion Detection Prevention System*).

Sistem dibuat dengan melalui tahap-tahap perencanaan, analisis, desain, dan implementasi. Analisis dilakukan pada objek penelitian yaitu *Yogya Crew/Indonesian Backtrack Team reg. Yogyakarta*. Perancangan sistem IDPS (*Intrusion Detection Prevention System*) yang digunakan pada penulisan ini adalah sistem yang tidak hanya mendeteksi ancaman tetapi memiliki kemampuan dalam melakukan pencegahan terhadap ancaman sebuah jaringan. Adanya sistem IDPS diharapkan dapat meningkatkan tingkat keamanan jaringan.

Kata-kunci : Keamanan jaringan, sistem IDPS, server, *scanning*, *Denial of Service(DoS)*.

ABSTRACT

In the current information technology development and data exchange information quickly is essential especially on a network connected to the Internet. Network security as part of a system is essential for maintaining the validity and integrity of the data and to ensure the authenticity of the data. However, a network security is often compromised by the threat from within or from outside. Variety of threats in the network just started doing tests on the network such as network scanning or making becomes paralyzed by launching a Denial of Service (DoS), to attempt to obtain important information from the server.

Administrators are fully responsible for the network security. It must be done continuously to maintain the quality of the network, due to errors in the network can not be detected when it happened. It is bad when a network error is not known as being a network administrator does not exist in the supervision. One method to monitor network security by implementing a system IDPS (Intrusion Detection Prevention System).

The system is made with through the stages of planning, analysis, design, and implementation. Analysis was performed on the object of research is Yogya Crew / Indonesian Backtrack Team reg. Yogyakarta. System design IDPS (Intrusion Detection Prevention System) which is used in this paper is a system that not only detects a threat but has the ability to take precautions against the threat of a network. The existence of IDPS system is expected to increase the level of network security.

Keywords: *Network security, systems IDPS, servers, scanning, Denial of Service (DoS).*