

**RANCANG MODEL SISTEM KEAMANAN JARINGAN
KOMPUTER MENGGUNAKAN *INTRUSION PREVENTION*
SYSTEM DENGAN METODE *RULE BASED* :
STUDI KASUS KPDE PROVINSI JAMBI**

TESIS



Oleh:

ABDUL RAHIM

1311601783

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2015

**RANCANG MODEL SISTEM KEAMANAN JARINGAN
KOMPUTER MENGGUNAKAN INTRUSION PREVENTION
SYSTEM DENGAN METODE RULE BASED :
STUDI KASUS KPDE PROVINSI JAMBI**

TESIS

**Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (MKOM)**



Oleh:

ABDUL RAHIM

1311601783

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

JAKARTA

2015



**PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama Mahasiswa : Abdul Rahim
Nomor Induk Mahasiswa : 1311601783
Program Studi : Magister Ilmu Komputer
Fakultas/Program : Pasca Sarjana

Menyatakan bahwa tesis yang berjudul :

**RANCANG MODEL SISTEM KEAMANAN JARINGAN KOMPUTER
MENGUNAKAN *INTRUSION PREVENTION SYSTEM* DENGAN
METODE RULE BASED : (STUDI KASUS KPDE PROVINSI JAMBI)**

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. Saya ijin untuk dikelola pihak Universitas Budi Luhur sesuai norma hukum dan etika yang berlaku

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila dikemudian hari pernyataan ini tidak benar.

Jakarta, 18 September 2015




Abdul Rahim)



**PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

LEMBAR PENGESAHAN

Nama Mahasiswa : Abdul Rahim
Nomor Induk Mahasiswa : 1311601783
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata Dua
Judul : Rancang Model Sistem Keamanan Jaringan Komputer
Menggunakan Intrusion Prevention System dengan Metode
Rule Based : Studi Kasus KPDE Provinsi Jambi

Jakarta, 8 Agustus 2015

Tim Penguji:

Ketua,
Prof. Dr. Moedjiono, M.Sc

Anggota,
Ir. Wendi Usino, MM, M.Sc, PhD

Pembimbing,
Dr. Ir. Nazori AZ, MT

Tanda Tangan

Ketua Program Studi

Dr. Ir. Nazori AZ, MT

ABSTRAK

NIM : 1311601783
Nama : Abdul Rahim
Judul Tesis : RANCANG MODEL SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN *INTRUSION PREVENTION SYSTEM* DENGAN METODE *RULE BASED* : (STUDI KASUS KPDE PROVINSI JAMBI)

Sistem keamanan komputer, dalam beberapa tahun ini telah menjadi fokus utama dalam dunia jaringan komputer, hal ini disebabkan tingginya ancaman yang mencurigakan dan serangan dari Internet. Keamanan komputer merupakan salah satu kunci yang dapat mempengaruhi tingkat *reliability*, termasuk *performance* dan *availability* pada suatu *internetwork*. Ancaman pada suatu jaringan komputer dapat berasal dari jaringan itu sendiri maupun dari jaringan internet, hal ini dapat disebabkan karena terdapat sumber daya yang bersifat publik sehingga untuk menjaga sumber daya yang ada pada jaringan komputer tersebut dibutuhkan suatu sistem khusus agar jaringan serta layanan-layanan yang terdapat pada jaringan tersebut tetap dapat digunakan dengan baik. Salah satu teknik untuk mengamankan sumber daya yang terdapat di jaringan komputer adalah dengan menggunakan *intrusion detection system (IDS)* atau sistem deteksi penyusup, dimana dengan adanya sistem deteksi penyusup, maka aktivitas jaringan yang mencurigakan dapat segera diketahui, selain itu dapat dilakukan tindakan pencegahan atau yang dikenal dengan nama *intrusion prevention system (IPS)*. Dalam tesis ini membahas tentang rancang model sistem keamanan menggunakan *intrusion prevention system* dengan metode *rule based* untuk melakukan pengamanan pada sumber daya jaringan komputer. Metode pengujian yang digunakan adalah metode pengujian *blackbox testing*, IDS akan diimplementasikan pada sistem operasi berbasis linux dan sistem pencegahan akan diimplementasikan pada *iptables* dan perangkat *router gateway*. Hasil dari penelitian ini berupa sistem pencegah penyusup (IPS) yang dapat meningkatkan keamanan sumber daya jaringan komputer dari ancaman baik yang berasal dari jaringan internet maupun intranet.

Kata Kunci : keamanan komputer, keamanan server, *intrusion detection system*, *intrusion prevention system*, keamanan jaringan komputer, sistem pencegahan.

ABSTRACT

NIM : 1311601783
Nama : Abdul Rahim
Judul Tesis : RANCANG MODEL SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN INTRUSION PREVENTION SYSTEM DENGAN METODE RULE BASED : (STUDI KASUS KPDE PROVINSI JAMBI)

Computer security systems, in recent years has become a major focus in the world of computer networks, this is due to the high threat of suspicious and attacks from the Internet. Computer security is one of the keys that can affect the level of reliability, including performance and availability on an internetwork. Threats to a computer network can be derived from the network itself or from the internet, this can be caused because there are public resources so as to maintain the existing resources in the computer network needs a special system to the network and the services that are on the network can still be used with either. One technique to secure the resources contained in a computer network is to use intrusion detection system (IDS) or intruder detection systems, where the presence of an intruder detection system, the suspicious network activity can be immediately known, but it can be done or that precautions known as intrusion prevention system (IPS). In this thesis discusses about the model design of security systems using intrusion prevention system with rule-based method for providing security in computer network resources. Testing method used is the method of testing blackbox testing, IDS will be implemented on a Linux-based operating system and prevention system will be implemented in iptables and gateway router device. The results of this study in the form of an intruder prevention systems (IPS) that can improve the security of computer network resources from threats originating from the Internet or intranet.

Keywords: Computer security, server security, intrusion detection systems, intrusion prevention systems, computer network security, the prevention system.

KATA PENGANTAR

Puji syukur penulis panjatkan atas kehadiran Tuhan Yang Maha Esa, karena berkat rahmat dan karunianya penulis dapat menyelesaikan tesis ini dengan judul “Rancang Model Sistem Keamanan Jaringan Komputer menggunakan Intrusion Prevention System Studi Kasus KPDE Provinsi Jambi” sebagai syarat melakukan tesis untuk memenuhi salah satu persyaratan memperoleh gelar Magister Ilmu Komputer pada Universitas Budi Luhur. Pada kesempatan ini penulis mengucapkan terima kasih kepada :

1. Bapak Dr. Moedjiono, M.Sc selaku Direktur Program Pascasarjana Universitas Budi Luhur.
2. Bapak Dr. Ir. Nazori AZ, MT selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur dan selaku Pembimbing Tesis.
3. Bapak Ir. Eddy Anthony, SH, MM selaku Ketua Yayasan Dinamika Bangsa Jambi dimana tempat penulis bekerja.
4. Bapak Dr. Ir. Herry Mulyono, MM selaku Pengurus Harian Yayasan Dinamika Bangsa Jambi dimana tempat penulis bekerja.
5. Seluruh Dosen Universitas Budi Luhur yang telah memberikan pengetahuan dan pengarahan selama penulis mengikuti pendidikan di Universitas Budi Luhur.
6. Seluruh Dosen STIKOM Dinamika Bangsa yang selalu meluangkan waktu untuk berdiskusi.
7. Seluruh pihak yang telah membantu baik secara langsung maupun tidak langsung hingga terselesaikannya tesis ini.

Penulis menyadari bahwa dalam tesis ini masih banyak kekurangannya, untuk itu penulis mengharapkan kritik dan saran untuk penyempurnaan yang akan datang. Akhir kata penulis mengucapkan terima kasih.

Jakarta, 18 September 2015
Penulis,

Abdul Rahim

DAFTAR ISI

LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN	ii
ABSTRAK	iii
ABSTRACT	iv
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Masalah Penelitian	2
1.2.1 Identifikasi Masalah	2
1.2.2 Pembatasan Masalah	3
1.2.3 Rumusan Masalah	3
1.3 Tujuan dan Manfaat Penelitian	3
1.3.1 Tujuan Penelitian	3
1.3.2 Manfaat Penelitian	3
1.4 Sistematika Penulisan	3
1.5 Daftar Pengertian	4
BAB II LANDASAN TEORI DAN KERANGKA KONSEP	5
2.1 Tinjauan Pustaka	5
2.1.1 Keamanan Jaringan Komputer	5
2.1.2 Tujuan Keamanan Jaringan Komputer	5
2.1.3 Ancaman Keamanan Jaringan Komputer	6
2.1.4 SQL Injection	8
2.1.5 Port Scanning	11
2.1.6 Model OSI	14
2.1.7 Port Logikal	16
2.1.8 Internet Protocol Address (IP)	18
2.1.9 Demilitarized Zone	19
2.1.10 Intrusion Detection System (IDS)	21
2.1.11 Intrusion Prevention Sistem (IPS)	25
2.1.12 Snort	26
2.1.12.1 Metode Rule based	29
2.1.12.2 Log Database Snort	31
2.1.13 Mikrotik RouterOS	32
2.1.14 Firewall	33
2.1.15 IPTables	35
2.1.16 Blackbox Testing	36
2.1.17 Pengujian Tingkat Deteksi dan Pencegahan	37
2.1.18 Data	37
2.2 Tinjauan Studi	38
2.3 Tinjauan Objek Penelitian	42

2.3.1	Sumber Daya Jaringan	42
2.3.2	Topologi Jaringan	43
2.4	Kerangka Konsep	45
2.5	Hipotesa Penelitian	46
BAB III METODOLOGI DAN RANCANGAN PENELITIAN		47
3.1	Metode Penelitian	47
3.2	Langkah Penelitian	47
3.3	Jadwal Penelitian	51
BAB VI PEMBAHASAN HASIL PENELITIAN		53
4.1	Analisa Sistem	53
4.1.1	Analisa Jaringan Komputer	53
4.1.1.1	Analisa Keamanan Jaringan Komputer	53
4.1.1.2	Analisa Topologi Jaringan Komputer	55
4.1.1.3	Analisa Layanan Jaringan Komputer	57
4.1.2	Perancangan Model Sistem Keamanan	58
4.1.2.1	Perancangan Topologi dan Demilitarized Zone	58
4.1.2.2	Perancangan Model Sistem Keamanan Deteksi	61
4.1.2.3	Perancangan Rules Based Snort	62
4.1.2.4	Perancangan Model Sistem Keamanan Pencegahan	65
4.2	Hasil Penelitian dan Pembahasan	67
4.2.1	Port Scanning	68
4.2.2	SQL Injection	68
4.2.3	Pengujian Non-Fungsional	69
4.3	Hasil Pengujian dan Evaluasi	69
4.3.1	Hasil Sampling Data	69
4.3.1.1	Location Clustering	70
4.3.1.2	Time Clustering	71
4.3.1.3	Technique Clustering	74
4.3.2	Hasil Kinerja Sistem Pencegahan	74
4.4	Implikasi Penelitian	75
4.4.1	Aspek Sistem	75
4.4.2	Aspek Manajerial	75
4.4.3	Aspek Penelitian Lanjut	75
4.5	Rencana Implementasi	75
BAB V PENUTUP		78
5.1	Kesimpulan	78
5.2	Saran	78
Daftar Pustaka		79
Lampiran-Lampiran		82
Riwayat Hidup		107

DAFTAR GAMBAR

Gambar	Halaman
II-1 Aspek CIA (Dony Ariyus, 2007 : 25)	6
II-2 Statistik Teknik Serangan September 2012.....	9
II-3 Aplikasi NMAP	13
II-4 Topologi DMZ.....	19
II-5 Gambar src-nat.....	20
II-6 Gambar dst-nat.....	21
II-7 Topologi IPS.....	25
II-8 Topologi IPS.....	26
II-9 Arsitektur Snort.....	27
II-10 Struktur Database Snort.....	31
II-11 Topologi firewall.....	34
II-12 Cara Kerja Firewall	35
II-13 IDS dan IPS berada dalam satu perangkat.....	41
II-14 Perangkat IDS dan Router Paket filtering	41
II-15 Topologi Jaringan Komputer KPDE Provinsi Jambi	44
III-16 Tahapan Penelitian.....	48
IV-1 Analisa Port Scanning.....	54
IV-2 Analisa Aplikasi Web	55
IV-3 Topologi Jaringan Komputer	56
IV-4 Perancangan Topologi Jaringan Komputer.....	59
IV-5 Flowchart Sistem Deteksi Penyusup	62
IV-6 Flowchart Sistem Pencegah Penyusup	66
IV-7 Grafik Lokasi Serangan	70
IV-8 Grafik Serangan bulan juni	73
IV-9 Grafik Serangan bulan agustus.....	73
IV-10 Grafik Serangan bulan agustus.....	73
IV-11 Grafik berdasarkan teknik serangan	74

DAFTAR TABEL

Tabel	Halaman
II-1 Port Logikal	17
II-2 IP Address versi 4	18
II-3 IP Private	18
II-4 Karakter Serangan SQL Injection	30
II-5 Ringkasan Tinjauan Studi	39
III-1 Jadwal Penelitian	51
IV-1 Data Serangan 2013-2014	54
IV-2 Alokasi Alamat IP	56
IV-3 Daftar layanan dan domain	57
IV-4 Alokasi Alamat IP DMZ	59
IV-5 Dst-nat	60
IV-6 Pengujian Port Scanning	68
IV-7 Pengujian SQL Injection	68
IV-8 Pengujian Kinerja IDS	69
IV-9 Data 26 Juni 2014 sampai 26 Agustus 2014	70
IV-10 Data lokasi Serangan	71
IV-11 Data Serangan dari jam 08:00-16:59	71
IV-12 Data Serangan dari jam 17:00-23:59	72
IV-13 Data Serangan dari jam 00:00-05:59	72
IV-14 Rata-rata serangan perhari	74

DAFTAR LAMPIRAN

Lampiran	Halaman
1. MySQL Trigger	82
2. cmd.php	83
3. ipt.sh	84
4. iptables-blocklist.txt	84
5. Firewall Filter	85
6. Sampel Data	88
7. Data Serangan berdasarkan lokasi	88
8. Data serangan bulan juni	89
9. Data serangan bulan juli	89
10. Data serangan bulan agustus	90
11. Skenario Port Scanning	92
12. Skenario SQL Injection	96
13. Data serangan tahun 2014	103
Riwayat Hidup	104

DAFTAR PUSTAKA

- [Abdul 2012] Abdul Rouf. "Pengujian Perangkat Lunak Dengan Menggunakan Metode White box dan Black box". Jurnal. STMIK Himsya Semarang, 2012.
- [Agus 2012] Agus Kurniawan. "Network Forensics". Andi Offset, Yogyakarta (2012).
- [Alamsyah 2008] Alamsyah. "Implementasi Keamanan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) menggunakan CLEAROS". Jurnal SMARTek, Vol.9 No.3. (Agustus, 2011) : 224-229.
- [Ariyus 2007] Dony Ariyus "Intrusion Detection System Sistem Pendeteksi Penyusup pada Jaringan Komputer". Yogyakarta : andi. 2007
- [Brennan 2014] Brennan, Michael P. "Using Snort For a Distributed Intrusion Detection System V1.3". Sans Institute InfoSec Reading Room, (2014)
- [Chris and Hunt 2005] Chris Brenton and Cameron Hunt. "Network Security". PT. Elex Media Komputindo (2005).
- [Cisco.com 2013] Cisco "Network Address Translation (NAT) FAQ". 2013. <http://www.cisco.com> (Diakses 10 Mei 2014).
- [Deris, 2013] Deris Stiawan. "Intrusion Prevention System (IPS) Tantangan dalam Pengembangannya". Artikel. Fasilkom, Universitas Sriwijaya, 2012.
- [Binh 2006] Duong, Binh, T "Comparisons Of Attacks On Honeypots With Those On Real Networks". 2006. <http://faculty.nps.edu> (Diakses 10 Mei 2014).
- [Egevang 1994] Network Group Working, IETF "The IP Network Address Translator (NAT)". 1994. <http://www.ietf.org/> (Diakses 10 Mei 2014).
- [Fydoor 1997] nmap.org "The Art of Port Scanning". 2014. http://nmap.org/nmap_doc.html (Diakses 10 Mei 2014).
- [Google.com 2011] google.com "Cara Kerja Firewall". 2011. <http://google.com> (Diakses 10 Mei 2014).
- [Highsec.es 2012] highsec.es "Topologi IPS". 2012. <http://highsec.es> (Diakses 10 Mei 2014).