

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

SKRIPSI

ANALISA SISTEM KEAMANAN IDS DENGAN METODE
SIGNATURE-BASED DAN PENCEGAHANNYA BERBASIS

FIREWALL



Diajukan Oleh:

- 1. AAN BAYUMI / 011090240**
- 2. ANUWAR / 012070111**
- 3. ZENDRI OKTARA / 011100172**

Untuk Memenuhi Sebagian Dari Syarat-Syarat

Guna Mencapai Gelar Sarjana Komputer

PALEMBANG

2014

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

HALAMAN PENGESAHAN PEMBIMBING

NAMA/NPM : 1. AAN BAYUMI /011090240
2. ANUWAR /012070111
3. ZENDRI OKTARA /011100172

PROGRAM STUDI : TEKNIK INFORMATIKA

JENJANG PENDIDIKAN : STRATA SATU (S1)

KONSENTRASI : JARINGAN

JUDUL SKRIPSI : ANALISA SISTEM KEAMANAN IDS
DENGAN METODE SIGNATURE-BASED DAN
PENCEGAHANNYA BERBASIS FIREWALL


Palembang, 17 September 2014

Menyetujui,

Pembimbing,

Mengetahui,

Ketua,


Gantoro Barovih, S.Kom., M.Kom
NUPN : 9932000056




Benedictus Effendi, S.T., M.T.
NIP : 09.PCT.13

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

HALAMAN PENGESAHAN PENGUJI

NAMA/NPM : 1. AAN BAYUMI / 011090240
2. ANUWAR / 012070111
3. ZENDRI OKTARA / 011100172

PROGRAM STUDI : TEKNIK INFORMATIKA

JENJANG PENDIDIKAN : STRATA SATU (S1)

KONSENTRASI : JARINGAN

JUDUL SKRIPSI : ANALISA SISTEM KEAMANAN IDS
DENGAN METODE SIGNATURE-BASED DAN
PENCEGAHANNYA BERBASIS FIREWALL

Tanggal, 4 September 2014

Penguji I,


Alfred Tenggono, S.Kom., M.Kom.

NUPN : 9902702078

Tanggal, 4 September 2014

Penguji II,


Salimin Bahar, S.Kom.

NIDN : 0215106902

Mengetahui,

Ketua,


Benedictus Effendi, S.T., M.T.

NIP : 09.PCT.13

Motto :

Tak akan pernah ada keberhasilan jika hanya diam dan berpangku tangan, berusaha dengan sungguh-sungguh sampai akhir karena kita tidak tau apa yang akan terjadi di masa yang akan datang.

Kupersembahkan Kepada :

- Kedua Orang Tua
- Karib- kerabat
- Keluarga besar
- Staff dan Seluruh Dosen STIMIK Palcomtech
- Seluruh Teman-teman

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
MOTTO DAN PERSEMBAHAN	iv
HALAMAN PERNYATAAN	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
ABSTRAK	xiii
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Perumusan Masalah	3
1.3 Ruang Lingkup.....	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan.....	4
BAB II GAMBARAN UMUM PERUSAHAAN	
2.1 Sejarah Perusahaan.....	6
2.2 Struktur Organisasi dan Uraian Tugas Wewenang	7
2.2.1 Struktur Organisasi.....	7
2.2.2 Tugas dan Wewenang	8
BAB III TINJAUAN PUSTAKA	
3.1 Landasan Teori.....	11
3.1.1 Analisis Sistem.....	11
3.1.2 Jaringan Komputer	12
3.1.3 Keamanan Komputer	13
3.1.4 <i>Intrusion Detection System (IDS)</i>	24
3.1.5 <i>Snort</i>	26
3.1.6 <i>Basic Analysis and Security Engine (BASE)</i>	28
3.2 Penelitian Terdahulu	30
3.3 Kerangka Penelitian	31
BAB IV METODE PENELITIAN	
4.1 Jadwal Penelitian.....	33
4.1.1 Tempat.....	33
4.1.2 Waktu	33
4.2 Teknik Pengumpulan Data.....	33
4.3 Teknik Pengembangan Sistem	34
4.4 Skema Pengujian.....	36

BAB V	HASIL DAN PEMBAHASAN	
5.1	Hasil	38
5.1.1	Analisis	38
5.1.1.1	Analisis Kebutuhan	38
5.1.1.2	Analisis Permasalahan	39
5.1.2	Desain Topologi Jaringan yang diusulkan	40
5.1.3	Implementasi dan konfigurasi <i>Sensor Snort</i>	41
5.2	Pengujian dan Pembahasan	49

BAB VI	KESIMPULAN DAN SARAN	
6.1	Kesimpulan	61
6.2	Saran.....	61

DAFTAR PUSTAKA

DAFTAR GAMBAR

Gambar	Halaman
Gambar 2.1 Struktur organisasi PT. Menara Nusantara Perkasa	8
Gambar 3.1 Kerangka Penelitian	32
Gambar 4.1 <i>Action Research Model</i>	35
Gambar 4.2 Cara kerja IDS	36
Gambar 4.3 Skema pengujian	37
Gambar 5.1 Topologi Jaringan yang diusulkan	41
Gambar 5.2 Installasi paket pendukung IDS.....	41
Gambar 5.3 Download web BASE dan Adodb.....	42
Gambar 5.4 Installasi Snort Mysql.....	42
Gambar 5.5 Membuat database.....	43
Gambar 5.6 Memasukan tabel snort ke database	43
Gambar 5.7 Tampilan tabel snort.....	44
Gambar 5.8 Konfigurasi snort.....	44
Gambar 5.9 Konfigurasi <i>rule_path</i>	45
Gambar 5.10 Mengaktifkan <i>log_unified</i>	45
Gambar 5.11 Konfigurasi Output Database	45
Gambar 5.12 Ekstrak File Base dan Adodb	46
Gambar 5.13 Memindahkan Base dan Adodb	46
Gambar 5.14 Tampilan Rule Snort	47
Gambar 5.15 Tampilan awal installasi snort base.....	47
Gambar 5.16 Konfigurasi path Adodb	48
Gambar 5.17 Konfigurasi <i>Database Base</i>	48
Gambar 5.18 Konfigurasi admin Base	49
Gambar 5.19 Tampilan login base snort	49
Gambar 5.20 Tampilan <i>trafik protocol Base</i>	50
Gambar 5.21 Tampilan <i>Sensor interface</i>	50
Gambar 5.22 Tampilan <i>Unique alerts</i>	51
Gambar 5.23 Tampilan <i>Categories</i> dan <i>unique alerts</i>	52
Gambar 5.24 Tampilan <i>display alert</i>	53
Gambar 5.25 Tampilan <i>display alert</i>	53
Gambar 5.26 Tampilan <i>Display Alert</i>	54
Gambar 5.27 Tampilan <i>Ping Attack</i>	54
Gambar 5.28 Tampilan <i>Scan Port</i>	55
Gambar 5.29 Tampilan serangan <i>flooding protocol tcp</i> dan <i>udp</i>	56
Gambar 5.30 Tampilan serangan Syn Attack	56
Gambar 5.31 Daftar IP Address yang melakukan serangan.....	57
Gambar 5.32 Perintah untuk <i>reject ping attack</i>	57
Gambar 5.33 Hasil penolakan <i>ping attack</i>	58
Gambar 5.34 Hasil Memblok serangan dos dan konfigurasi Iptables	58
Gambar 5.35 Kegagalan serangan <i>dos (flooding)</i>	59
Gambar 5.36 Kegagalan serangan <i>syn attack</i>	59

DAFTAR TABEL

TABEL	Halaman
Tabel 3.1 Perbedaan NIDS dan HIDS.....	25
Tabel 4.1 Skenario Pengujian	37
Tabel 5.1 Tabel keberhasilan pengujian.....	60

ABSTRAK

Cara untuk menjaga keamanan sebuah sistem yang dapat meminimalisasi serangan-serangan terhadap jaringan LAN (*Local Area Network*) bahkan *server* dari penyusup ini yaitu menggunakan alat deteksi yang berfungsi untuk mendeteksi terjadinya intrusi pada sistem server jaringan. Alat deteksi yang dimaksud adalah *Intrusion Detection System (IDS)*. *Knowledge-based (signature-based)* IDS dapat mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan *database rule* IDS (berisi *signature - signature* paket serangan) . Jika paket data mempunyai pola yang sama dengan (setidaknya) salah satu pola di *database rule* IDS, maka paket tersebut dianggap sebagai serangan, dan demikian juga sebaliknya, jika paket data tersebut sama sekali tidak mempunyai pola yang sama dengan pola di *database rule* IDS, maka paket data tersebut dianggap bukan serangan. Kemudian *IDS engine* akan membaca *alert* dari IDS (antara lain berupa jenis serangan dan *IP address* penyusup) untuk kemudian memerintahkan *firewall* untuk memblok akses koneksi ke sistem dari penyusup tersebut

Keyword: *Intrusion Detection System, Knowledge-based, Log, rule, engine*

KATA PENGANTAR

Segala puji hanya milik Allah SWT. Shalawat dan salam selalu tercurahkan kepada Rasulullah SAW. Berkat limpahan dan rahmat-Nya penyusun mampu menyelesaikan lapoan Skripsi yang berjudul “ Analisa Sistem Keamana Intrusion Detection System (IDS) Dengan metode Signature-based dan pencegahan Berbasis Firewall di PT. Menara Nusantara Palembang”.

Dalam penyusunan laporan Skripsi ini, tidak sedikit hambatan yang penulis hadapi. Namun penulis menyadari bahwa kelancaran dalam penyusunan materi ini tidak lain berkat bantuan, dorongan, dan bimbingan orang tua, sehingga kendala-kendala yang penulis hadapi teratasi.

Semoga laporan ini dapat memberikan wawasan yang lebih luas dan menjadi sumbangan pemikiran kepada pembaca khususnya para mahasiswa STMIK Palcomtech. Saya sadar bahwa laporan ini masih banyak kekurangan dan jauh dari sempurna.

Untuk itu, kepada dosen pembimbing saya meminta masukannya demi perbaikan pembuatan lapoan saya di masa yang akan datang dan mengharapkan kritik dan saran dari para pembaca.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Banyak manfaat dan keuntungan yang diperoleh melalui penggunaan jaringan komputer untuk melakukan aktivitas-aktivitas terutama penggunaan internet, maka semakin banyak pula pemakai komputer yang menghubungkan komputernya dengan internet, tentunya masalah keamanan menjadi semakin rumit dalam penanganannya. Oleh karena itu sistem keamanan ini seharusnya menjadi pertimbangan untuk menggunakan internet sebagai media koneksinya.

PT. Menara Nusantara Perkasa bergerak dibidang distribusi *retail* yang melayani beberapa perusahaan besar maupun kecil yang tersebar diberbagai wilayah Sumatera Selatan baik didalam maupun luar kota. Adapun kendala yang ada pada perusahaan dalam hal keamanan jaringan, dimana dalam *file log* sering kali terdapat *ip address* atau identitas penyusup yang mencoba mengambil kendali server menggunakan akses *root* ke server pusat database perusahaan. *Log* adalah sebuah file yang berisi daftar tindakan, kejadian (aktivitas) yang telah terjadi di dalam suatu sistem jaringan komputer. Oleh karena itu penulis mencoba melakukan evaluasi dan pencegahan terhadap ancaman tersebut.

Salah satu solusi dari permasalahan tersebut adalah diperlukan cara untuk menjaga kewanaman sebuah sistem yang dapat meminimalisasi

serangan-serangan terhadap jaringan LAN (*Local Area Network*) bahkan *server* dari penyusup ini. Alat deteksi sangat diperlukan dalam kondisi ini, yang dapat mendeteksi terjadinya intrusi pada sistem server jaringan. Alat deteksi yang dimaksud adalah *Intrusion Detection System* (IDS). *Knowledge-based (signature-based)* IDS dapat mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan *database rule* IDS (berisi *signatur-signature* paket serangan). Jika paket data mempunyai pola yang sama dengan (setidaknya) salah satu pola di *database rule* IDS, maka paket tersebut dianggap sebagai serangan, dan demikian juga sebaliknya, jika paket data tersebut sama sekali tidak mempunyai pola yang sama dengan pola di *database rule* IDS, maka paket data tersebut dianggap bukan serangan. Kemudian *IDS engine* akan membaca *alert* dari IDS (antara lain berupa jenis serangan dan *IP address* penyusup) untuk kemudian memerintahkan *firewall* untuk memblokir akses koneksi ke sistem dari penyusup tersebut.

Berdasarkan latarbelakang di atas, penulis tertarik untuk membuat penelitian dengan judul “ Analisa Sistem Keamanan *Intrusion Detection System* (IDS) dengan metode *Signature-based* dan pencegahannya berbasis *firewall* di PT. Menara Nusantara Perkasa”

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas pada penelitian ini adalah bagaimana merancang dan menganalisa sistem pengamanan jaringan komputer pada *Intrusion Detection System* (IDS) dengan menggunakan metode *signature-based* ?

1.3 Ruang Lingkup

Ruang lingkup permasalahan *Intrusion Detection System* (IDS) sangatlah luas, maka dalam penulisan skripsi ini penulis lebih menekankan pada analisis serangan berdasarkan data-data yang dihasilkan oleh sensor IDS yang dikenali sebagai penyusup/penyerang dengan menggunakan metode *Signature-based*.

1.4 Tujuan Penelitian

Adapun Tujuan penelitian adalah sebagai berikut

- a. Menerapkan sistem keamanan jaringan LAN dengan melakukan implementasi *Intrusion Detection System* (IDS) dan pencegahannya berbasis *Firewall* di PT. Menara Nusantara Perkasa.
- b. Untuk mengetahui dan menganalisa paket-paket data yang melalui sistem *BASE* (*Basic Analysis and Security Engine*) dengan menggunakan metode *signed-based*.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah

- a. Dapat meningkatkan keamanan jaringan LAN di PT. Menara Nusantara Perkasa terutama keamanan server jaringan.

- b. Dapat menerapkan mata kuliah Praktik Jaringan Komputer (PJK) yang telah didapat selama mengikuti perkuliahan pada STMIK PalComTech.
- c. Dari hasil penelitian ini diharapkan dapat menjadi bahan *referensi* untuk mahasiswa STMIK PalComTech untuk penelitian selanjutnya.

1.6 Sistematika Penulisan

Skripsi ini ditulis dalam Enam bab dan masing-masing bab terbagi dalam sub-sub bab. Sistematika penulisan skripsi ini disusun sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini Penulis akan menguraikan tentang latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II GAMBARAN UMUM PERUSAHAAN

Pada bab ini menjelaskan tentang sejarah perusahaan, struktur organisasi, wewenang dan tanggung jawab karyawan perusahaan dan kegiatan kerja yang dilakukan.

BAB III TINJAUAN PUSTAKA

Pada bab ini menjelaskan pembahasan mengenai landasan teori yang berkaitan dengan pokok permasalahan dalam penelitian.

BAB IV METODE PENELITIAN

Dalam bab ini membahas waktu penelitian, jenis data, teknik pengumpulan data dan Metode penelitian.

BAB V HASIL DAN PEMBAHASAN

Dalam bab ini membahas mengenai hasil dari penelitian yang telah dilakukan dan membahas mekanisme penelitian yaitu implementasi dan pengujian.

BAB IV PENUTUP

Menguraikan beberapa kesimpulan dari pembahasan masalah serta memberikan saran yang bermanfaat.

DAFTAR PUSTAKA

- Ariyus Dony. 2006. *Computer security*. Yogyakarta:ANDI.
- Ariyus, Dony. 2007. *Intrusion Detection System*. Yogyakarta: ANDI
- Herlambang Linto, Catur Azis. 2008. *Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik RouterOS*. Yogyakarta:ANDI.
- Hidayat, Aziz. 2011. *Metode Penelitian*. Penerbit Salemba Medika
- Jogiyanto. 2009. *Analisis dan Desain Sistem Informasi*. Penerbit Yogyakarta:ANDI
- Kock, Ned. 2007. *Information systems Action Research An Applied View Of emerging Concepts and Methods*. Texas A & M International University. USA
- Kumar, Vinod & Sangwan, Prakash (*International Journal of Computer Application & Information Technology Vol I, Issue III, November 2012*), *Signature Based Intrusion Detection System Using Snort*
- Nazir, Moh. 2003. *Metodologi Penelitian*. Bogor: Ghalia Indonesia
- Sugiantoro, Bambang & Istianto, Jazi (*Seminar Nasional Informatika 2 Mei 2010*). *Analisa sistem keamanan Intrusion Detection System (IDS), Firewall System, Database System dan Monitoring System menggunakan Agent bergerak*.
- Syarizal, Melwin. 2005. *Pengantar Jaringan Komputer*. Yogyakarta:ANDI