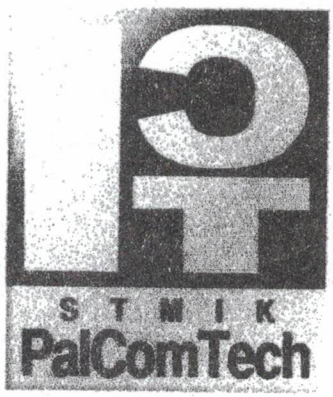
KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

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,	**Mengetahui,**
Pembimbing,	**Ketua,**
Guntoro Barovih, S.Kom.,M.Kom	**Benedictus Effendi, S.T.,M.T.**
NUPN : 9932000056	**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

DAFTAR GAMBAR

Gambar **Halaman**

DAFTAR TABEL

TABEL **Halaman**

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 pembu atan 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 kemanan 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 memblok 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 *signatured-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 Apllication & 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