SMARTek
SIPIL◇ MESIN ◇ARSITEKTUR ◇ELEKTRO

IMPLEMENTASI KEAMANAN INSTRUSION DETECTION SYSTEM (IDS) DAN INSTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN CLEAROS

*Alamsyah**

Abstract

As the current development of information technology is always changing, demanding the security of information is very important, especially on a network that connected to the Internet. But that is quite unfortunate is the imbalance between each of the development of a technology is not accompanied by progress on the security system itself. Thus quite a lot of systems are still weak and should be improved safety.

Security of a network is often interrupted by threats from within or from outside. The attack is a hacker attack that mean to spoil the Network Computer is connected to the internet or steal important information that exist on the network. The presence of a firewall has a lot of help in security, but with today's technologically developed only with security firewalls are yet to be fully guaranteed. Because it has developed technology IDS and IPS as an auxiliary safety data on a computer network. With the IDS and IPS, the more the attacks can be prevented or eliminated. IDS is useful for detecting the presence of an intruder attacks (attacks from within), while the IPS is useful to detect and follow up by blocking attacks (filter) attacks.

Key words : *Instrusion Detection System (IDS), Instrusion Prevention System (IPS), Firewal*

Abstrak

Seiring dengan Perkembangan Teknologi Informasi menjadikan keamanan suatu informasi sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan internet. Namun yang cukup disayangkan adalah ketidakseimbangan antara setiap perkembangan suatu teknologi tidak diiringi dengan perkembangan pada sistem keamanan itu sendiri, dengan demikian cukup banyak sistem-sistem yang masih lemah dan harus ditingkatkan keamanannya. Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar. Serangan tersebut berupa serangan Hacker yang bermaksud merusak Jaringan Komputer yang terkoneksi pada internet ataupun mencuri informasi penting yang ada pada jaringan tersebut. Hadirnya firewall telah banyak membantu dalam pengamanan, akan tetapi seiring berkembang teknolgi sekarang ini hanya dengan firewall keamanan tersebut belum dapat dijamin sepenuhnya. Karena itu telah berkembang teknologi *IDS* dan *IPS* sebagai pembantu pengaman data pada suatu jarigan komputer. Dengan adanya *Intrusion Detection System* (IDS) dan *Instrusion Prevention System* (IPS), maka serangan-serangan tersebut lebih dapat dicegah ataupun dihilangkan. IDS berguna untuk mendeteksi adanya serangan dari penyusup (serangan dari dalam), sedangkan IPS berguna untuk mendeteksi serangan dan menindaklanjutinya dengan pemblokan (filter) serangan.

Kata Kunci : *Instrusion Detection System (IDS), Instrusion Prevention System (IPS), Firewal*

1. Pendahuluan

Teknologi firewall sebagai tembok penghalang dalam kejahatan Internet dirasa tidak selalu efektif terhadap percobaan intrusi. Karena biasanya firewall dirancang hanya untuk memblokir *traffic* mencurigakan tanpa membedakan mana traffic yang berbahaya dan mana yang tidak berbahaya sehingga semua paket yang di anggap mengancam lansung di

* Staf Pengajar Jurusan Teknik Elektro Fakultas Teknik Universitas Tadulako, Palu

tindaki, akibatnya seorang admin dapat tertipu terhadap beberapa serangan yang tidak dapat diklasifikasikan. Begitu juga dengan prosedur untuk mengizinkan paket untuk lewat jika sesuai dengan *policy* dari *firewall*. Masalahnya adalah banyak program *exploit* konsentrasi serangannya memanfaatkan firewall. Sebagai contoh, percobaan attacker untuk melakukan penetrasi melalui port 23 (Telnet). Tetapi *policy* dari *firewall* memblokir permintaan untuk port 23. Mungkin attacker tidak bisa melakukan telnet ke komputer target karena rule dari firewall yang ketat. Tetapi firewall ternyata mengizinkan request (permintaan) dari luar untuk port 80 (http). Dan attacker dapat memanfaatkan port 80 untuk eksploitasi http. Ketika webserver telah berhasil dikuasai, firewall dapat dikatakan sudah di-bypass dan tidak berguna lagi.

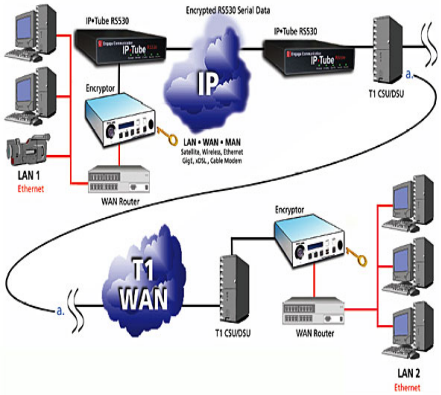
Dengan menggunakan sistem keamanan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) yang digunakan sebagai pelengkap teknologi keamanan dimana sistem pertahanan akan dapat mengambil tindakan sesuai dengan data pengklasifikasian yang jelas dan dapat menidaklanjuti laporan dari data yang sudah valid .

2. Tinjauan Pustaka

2.1 Jaringan komputer

Menurut Iwan Sofana:2008, Jaringan komputer *(computer networks)* adalah suatu himpunan inter koneksi sejumlah komputer autonomus. Dalam bahasa yang populer dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel *(nirkabel)* informasi berupa data akan mengalir dari satu komputer ke komputer lainnya sehingga masing-masing komputer yang terhubung tersebut bisa saling bertukar data dan informasi." *(iwan sovana/, 2008:3)*

Menurut Tom Thomas:2004, Klasifkasi jaringan komputer dibagi berdasarkan skala (LAN, WAN, MAN), topologi (*bus, star, ring, tree, mesh*), arsitektur (*client server, peer to peer, hybrid*).



Gambar 1. *Jaringan WAN*

2.2 Konsep Dasar *Intrusion Detection System* (IDS)

Menurut Onno Purbo:2010, IDS adalah usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal *cracker*) atau seorang *user* yang sah tetapi menyalahgunakan (*abuse*) sumberdaya sistem.

IDS merupakan program atau aplikasi yang dapat mendeteksi adanya gangguan pada sistem kita. Pada saat ini ada beberapa *Intrusion* /DS yang umum digunakan pada jaringan, salah satunya adalah SNORT. Adapun tujuan dari *tools* ini

diantaranya: mengawasi jika terjadi penetrasi kedalam sistem, mengawasi traffic yang terjadi pada jaringan, mendeteksi anomali terjadinya penyimpangan dari sistem yang normal atau tingkah laku user, mendeteksi signature dan membedakan pola antara *signature user* dengan attacker.

IDS juga memiliki cara kerja dalam menganalisa apakah paket data yang dianggap sebagai intrusion oleh intruser. Cara kerja IDS dibagi menjadi dua, yaitu:

a. Knowledge Based

Knowledge Based pada IDS adalah cara kerja IDS dengan mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan database rule pada IDS tersebut. Database rule tersebut dapat berisi signature-signature paket serangan. Jika pattern atau pola paket data tersebut terdapat kesamaan dengan rule pada database rule pada IDS, maka paket data tersebut dianggap sebagai serangan dan demikian juga sebaliknya, jika paket data tersebut tidak memiliki kesamaan dengan rule pada database rule pada IDS, maka paket data tersebut tidak akan dianggap serangan.

b. Behavior Based

Behavior Base adalah cara kerja IDS dengan mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan-kejanggalan pada sistem, aatu adanya keanehan dan kejanggalan dari kondiri pada saat sistem normal, sebagai contoh: adanya penggunaan memory yang melonjak secara terus menerus atau terdapatnya koneksi secara paralel dari satu IP dalam jumlah banyak dan dalam waktu yang bersamaan. Kondisi tersebut dianggap kejanggalan yang selanjutnya oleh IDS Anomaly Based ini dianggap sebagai serangan.

2.3 *Intrusion Prevention System (IPS)*

IPS merupakan jenis metode pengamanan jaringan baik software atau hardware yang dapat memonitor aktivitas yang tidak diinginkan atau intrusion dan dapat langsung bereaksi untuk untuk mencegah aktivitas tersebut. IPS merupakan pengembangan dari dari IDS. Sebagai pengembangann dari teknologi firewall, IPS melakukan kontrol dari suatu sistem berdasarkan aplikasi konten atau pattern, tidak hanya berdasarkan ports atau IP address seperti firewall umumnya. IDS Selain dapat memantau dan monitoring, IPS dapat juga mengambil kebijakan dengan memblock paket yang lewat dengan cara 'melapor' ke firewall.

Ada beberapa metode IPS melakukan kebijakan apakah paket data yang lewat layak masuk atau keluar dalam jaringan tersebut.

a. Signature-based Intrusion Detection System

Pada metode ini, telah tersedia daftar signature yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini akan melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem

jaringan komputer, data signature yang ada harus tetap ter-update.

b. *Anomaly-based Intrusion Detection System*

Pada metode ini, terlebih dahulu harus melakukan konfigurasi terhadap IDS dan IPS, sehingga IDS dan IPS dapat mengatahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Sebuah paket anomali adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut. Apabila IDS dan IPS menemukan ada anomali pada paket yang diterima atau dikirimkan, maka IDS dan IPS akan memberikan peringatan pada pengelola jaringan (IDS) atau akan menolak paket tersebut untuk diteruskan (IPS). Untuk metode ini, pengelola jaringan harus terus-menerus memberi tahu IDS dan IPS bagaimana lalu lintas data yang normal pada sistem jaringan komputer tersebut, untuk menghindari adanya salah penilaian oleh IDS atau IPS.

Intrussion prevenstion system mengkombinasikan kemampuan network based IDS dengan kemampuan firewall, sehingga selain mendeteksi adanya penyusup juga bisa menindaklanjuti dengan melakukan pengeblokan terhadap IP yang melakukan serangan. Beberapa IPS opensource yang dikenal yaitu: portsentry, sshdfilter, dan snort.

2.4 *Snort*

Snort merupakan sebuah produk terbuka yang dikembangkan oleh Marty Roesch dan tersedia gratis di www.snort.org. Snort bisa digunakan pada sistem operasi Linux, Windows, BSD, Solaris dan sistem operasi lainnya. Snort merupakan IDS berbasis jaringan yang menggunakan metode deteksi rule based, menganalisis paket data apakah sesuai dengan jenis serangan yang sudah diketahui olehnya. Snort digunakan karena memiliki beberapa kelebihan berikut: mudah dalam konfigurasi dan penambahan aturan-aturan, gratis, dapat berjalan pada sistem operasi yang berbeda-beda.

2.5 *ClearOS*

ClearOS adalah Linux yang di kostumasi khusus untuk keperluan server. Dengan berbagai fitur yang powerfull dan setting yang simple, ClearOS menjadi alternative pilihan, baik untuk pemula yang tidak mengerti linux sama sekali maupun untuk professional yang memerlukan kemampuan terbaik dari OS linux server. ClearOS diturunkan dari Linux CentOS yang mana merupakan clonningan dari Red Hat Enterprise Linux yang berbayar. ClearOS free, gratis dan lisensinya open source, jadi bisa dipakai kapanpun dan dimanapun tanpa terkendala legalisasi. Hal yang membuat segalanya mudah di ClearOS adalah cara settingnya yang via webconfig. ClearOS memiliki sourse base yang kuat dan stabiluntuk dijalankan sebagai server di warnet, game online, kantor-kantor, dan perusahaan. Keunggulan ClearOS diantaranya adalah sebagai berikut: open source, dukungan profesional, dan kemudahan setting.

3. Metode Penelitian

3.1 Rancangan penelitian

Pada penelitian ini, terdapat beberapa metode pengumpulan data yang digunakan, yaitu:

a. Metode kepustakaan

Metode pengumpulan data kepustakaan dilakukan dengan mengumpulkan data-data dari sumber atau buku yang relevan terhadap penelitian.

Gambar 2. *ClearOS*

b. Pembuatan program aplikasi

Pada tahap ini dilakukan konfigurasi aplikasi sistem IDS dan *IPS snort* dengan menggunakan Sistem Operasi ClearOS.

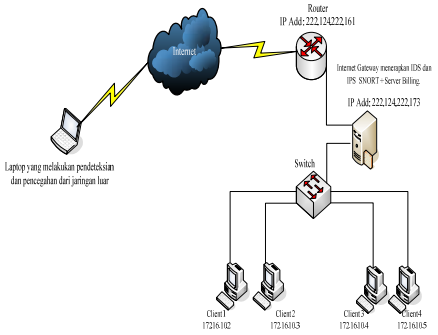
3.2 Sistem yang berjalan

Sistem Jaringan Internet pada umumnya yang ada saat ini memiliki router dan server yang memiliki IP Address Public sendiri-sendiri. Dengan adanya IP Public dapat menimbulkan adanya port-port yang terbuka pada Server, dari port-port yang terbuka dalam melakukan akses Internet dapat menimbulkan Serangan atau ancaman ke server tersebut.

3.3 Usulan pemecahan

Adapun usulan yang ditawarkan dalam mengatasi permasalahan pada sistem yg berjalan adalah menambahkan aplikasi Snort sebagai IDS dan IPS pada Internet Gateway.

Hal ini akan menjadikan ClearOS sebagai server multifungsi yang baik dan handal karena dapat memonitoring komputer server dan melakukan peringatan melalui *report trafic* apabila ada penyusup.



Gambar 3. Usulan Penambahan IDS dan IPS Snort pada Server Internet Gateway

4. Hasil dan Pembahasan

Dalam tahapan proses pembuatan aplikasi implementasi IDS dan IPS SNORT menggunakan ClearROS, tahapan yang paling penting adalah dengan melakukan konfigurasi. Konfigurasi ini di lakukan untuk memulai mengakses ClearOS berbasis *grafis user interface* (GUI).

a. Penginstalan ClearOS

Dari penginstalan ClearOS yang dilakukan maka diperoleh hasil seperti gambar 4.

Gambar 4. Tampilan Login Admin

b. Pemilihan Paket Bahasa

Setelah penulis memasukan username dan password maka akan muncul gambar untuk pemilihan bahasa seprti pada gambar 5.

Gambar 5. Pemilihan Paket Bahasa

c. Konfigurasi DNS Server

Selanjutnya memasukkan DNS server (dari IPS) seperti yg terlihat pada gambar 6 di bawah ini.

Gambar 6. Konfigurasi DNS Server

d. Pemilihan zona waktu

Selanjutnya akan muncul gambar zona waktu, dimana dalam menu ini akan dipilih tanggal, jam dan waktu setempat yang digunakan. Seperti yg terlihat pada gambar 7 di bawah ini.

Gambar 7. Pemilihan Zona Waktu

e. Pengisian nama organisasi

Sesaat kemudian akan muncul gambar untuk nama organization, dimana dalam menu ini akan dipilih sesuai data yg ada. Seperti yg terlihat pada gambar 8 di bawah ini.

Gambar 8. Pengisian Nama Organisasi

f. Proses konfigurasi selesai

Detelah melalui tahapan proses konfigurasi akan muncul gambar yg menerangkan bahwa proses telah selesai dan lanjut ke sistem selanjutnya. Seperti yg terlihat pada gambar 9.

Gambar 9. Proses Konfigurasi Selesai

5. Kesimpulan

Setelah melakukan proses tahapan pembuatan aplikasi IDS dan IPS Snort menggunakan ClearOS pada server dan client, maka dapat ditarik kesimpulan sebagai berikut:

a. Penerapan IDS (*Intrusion Detection System*) dan Penerapan IPS *(Intrusion Prevention System)* menggunakan Snort dapat mengawasi *traffic* yang terjadi pada jaringan Internet Universitas Tadulako Palu.
b. Penerapan IDS (*Intrusion Detection System*) dan IPS *(Intrusion Prevention System)* menggunakan Snort dapat mendeteksi dan mencegah anomaly pada sistem komputer server dari penyusup.
c. IDS (*Intrusion Detection System*) dan IPS *(Intrusion Prevention System)* menggunakan Snort dapat memonitoring traffic pada komputer server dan menyimpan hasil deteksi dan pencegah jika ada penyusup yang memasuki sistem komputer server.

6. Daftar Pustaka

Sopandi, Dede, 2010. *Membangun Jaringan Komputer*. Elex Media Komputindo. Jakarta

Cox, Kerry, 2004. *Managing Security With Snort and IDS Tools*. O'Reilly Media Inc. United States of America.

Deris, Setiawan, 2005. *Sistem Keamanan Komputer*. Elex Media Komputindo. Jakarta

Purbo, Onno, 2010. *Keamanan Jaringan Komputer*. Handry Pratama. Jakarta

Ardiyanto, Yudhi, 2010. *System Instrusion Detection System*. Sourcefire Inc. United States of America.

Thomas, Tom, 2004. *Network Security First*-.Step. Andi Offset. Yogyakarta