IMPLEMENTASI IDS (*INTRUSION DETECTION SYSTEM*) PADA SISTEM KEAMANAN JARINGAN SMAN 1 CIKEUSAL

Sutarti[1], Adi Putranto Pancaro[2], Fembi Isnanto Saputra[3]
Program Studi Sistem Komputer Fakultas Teknologi Informasi Universitas Serang Raya
sutarti86@gmail.com[1], adiputrantopancaro@gmail.com[2], fembiisnanto@gmail.com[3]

Abstrak – Seorang pengelola *server* jaringan dan internet (*system administrator*) memiliki tanggung jawab terhadap keamanan sistem dari waktu ke waktu, memastikan bahwa sistem dan jaringan yang dikelola terjaga dari berbagai peluang ancaman. Sekolah merupakan salah satu tempat dimana penggunaan jaringan internet terbuka terhadap pemakai-pemakainya. Penggunaan tersebut bisa dipergunakan dengan benar dan tidak pula disalahgunakan pemakaiannya. Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi. Sistem yang hanya mendeteksi ini akan diimplementasikan dengan menggunakan aplikasi *Intrusion Detection System* (IDS) yaitu *Snort* dan *PfSense* (*Router* OS) sebagai penindak lanjutnya terhadap *alert snort* yang dihasilkan. Berdasarkan percobaan serangan dengan komputer yang terpasang *snort* dapat mengetahui apa yang sedang terjadi yang di hasilkan pada *alert* seperti serangan *Ping Of Death* dan *Port Scan*. Pada *PfSense* menampilkan *alert* jika ada seseorang yang mencoba menyalahgunakan jaringan seperti mengakses sosial media *facebook*, *youtube*, *twitter* dan lain-lain bisa menindak lanjuti dengan mem-*block* secara otomatis.

Kata Kunci: *Alert, IDS, PfSense, Snort*

I. PENDAHULUAN

Pada era global saat ini, Teknologi Informasi (TI) telah berkembang dengan pesat, terutama dengan adanya jaringan internet yang dapat memudahkan dalam melakukan komunikasi dengan pihak yang lain. Dengan mudahnya pengaksesan terhadap informasi tersebut menyebabkan timbulnya masalah baru yaitu informasi atau data-data penting dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan sendiri. Sehingga suatu sistem keamanan jaringan menjadi salah satu aspek yang penting.

Seorang pengelola *server* jaringan dan internet (*system administrator*) memiliki tanggung jawab terhadap keamanan sistem dari waktu ke waktu, memastikan bahwa sistem dan jaringan yang dikelola terjaga dari berbagai peluang ancaman. Sekolah merupakan salah satu tempat dimana penggunaan jaringan internet terbuka terhadap pemakai-pemakainya. Penggunaan tersebut bisa dipergunakan dengan benar dan tidak pula disalahgunakan pemakaiannya. Hal ini mengakibatkan suatu sistem jaringan yang seharusnya digunakan sebagai pembelajaran akan tetapi disalahgunakan penggunaannya untuk aktifitas lain seperti mengakses jejaring sosial. Selain itu administrator harus mengetahui sesuatu *log* yang mengindentifikasi adanya serangan atau penyalahgunaan jaringan.

Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi yaitu dengan menggunakan aplikasi *Intrusion Detection System* (IDS) yaitu *Snort* dan *PfSense* (*Router* OS) sebagai penindak lanjut terhadap *alert snort* yang dihasilkan.

Tujuan yang akan dicapai dalam penelitian ini adalah:

1. Untuk mengetahui sebuah sistem *Intrusion Detection System* (IDS) *snort* dapat mendeteksi adanya serangan dan penyalahgunaan jaringan
2. Untuk mengetahui penganalisaan *log* yang dihasilkan sebagai peringatan kepada *administrator.*
3. Untuk mengetahui *PfSense* dapat melakukan tindakan lanjut terhadap *alert* yang dihasilkan oleh *snort.*

II. KAJIAN PUSTAKA

Riadi, I. (2011). Berdasarkan penelitian yang telah dilakukan aplikasi *router* menggunakan Mikrotik yang dihasilkan dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran aplikasi sesuai dengan kebutuhan pengguna. Permasalahan tersebut dapat diatasi menggunakan Mikrotik sebagai pengatur lalu lintas data internet serta melakukan pem-*filter*-an beberapa aplikasi yang dapat mengganggu konektifitas jaringan komputer sesuai dengan aturan yang telah ditetapkan.

Santoso. dkk. (2011). IDS/IPS StratGuard mampu berjalan di semua *platform* sistem operasi dan mampu menggantikan peranan *firewall* dan *proxy* sehingga bisa dilakukan pencegahan pada saat *intruder* melakukan penetrasi. IDS merupakan salah satu opsi untuk meningkatkan keamanan jaringan dalam sebuah *network* baik intranet maupun internet.

Gobel. Dkk. (2014). Penelitian dilakukan berdasarkan beberapa literatur yang membahas secara detail tentang aplikasi sistem *monitoring* terhadap aliran data dan distribusi informasi menggunakan SMS *gateway*. Pendekatan dilakukan dengan mengintegrasikan aplikasi berbeda untuk melakukan *real-time report* kepada *administrator* tanpa harus selalu ada di depan layar monitor, jika ada sesuatu peringatan ancaman bisa diterima melalui SMS. Dari hasil penelitian ini dapat disimpulkan bahwa peningkatan sikap *self protection* dapat dilakukan dengan sistem peringatan yang dapat memberikan laporan peringatan secara berkala. Hal ini tentu diharapkan juga dapat mengurangi beban kerja *administrator* yang tidak harus setiap saat melakukan pengecekan langsung terhadap sistem. Di sisi lain sistem ini dapat diterapkan sebagai alternatif sistem keamanan tambahan pada sistem dengan pengamanan yang parsial.

Hakim, A. dkk. (2014). IPS merupakan perkembangan dari IDS dimana pada IPS ini menggunakan *Suricata* sebagai pendeteksi penyusup dan dikoneksikan dengan *IPTables* sebagai pencegah penyusupan. IPS ini dilengkapi dengan tampilan (GUI) untuk memudahkan *admin* dalam memantau jaringan dari tindakan penyusupan kepada *server*. *Suricata* membuat *alert* ketika terdeteksi adanya penyusupan pada jaringan dan disimpan pada *file log Suricata*. Pada saat yang sama *WebAdmin* menampilkan dialog *alert* disertai dengan bunyi alarm dan memerintahkan *IPTables* untuk memblokir alamat IP yang teridentifikasi sebagai penyusup, sehingga akses penyerang terhadap *server* terputus. Berdasarkan percobaan yang telah dilakukan sebanyak 50 kali, *Suricata* dan *IPTables* dapat bekerja secara optimal dan mampu mendeteksi serangan.

Sumardi. dan Triyono, R. A. (2013). Penyebaran *malware* dan serangan dari luar yang bertujuan memperlambat jaringan dari internet dapat diminimalkan dengan cara *blocking port. WinBox* aplikasi untuk *remote desktop* basis GUI untuk mengatur *port* yang akan di *blocking*. Hasilnya setelah penerapan virus yang masuk melalui internet berkurang, jaringan yang sering *down* lebih jarang *down*, jaringan dan koneksi internet lebih stabil. Metode ini dapat meminimalkan risiko masuknya *malware* dan serangan dari luar yang dapat memicu terjadinya kelumpuhan jaringan lokal.

Rudi Hermawan (2011). Mengemukakan banyak alat dan teknik penyerang digunakan untuk menumbangkan target sistem keamanan. Kadang kala, keamanan dari sebuah sistem atau jaringan akan menggagalkan penyerang yang tidak ahli. Merasa frustasi dan tidak berdaya, penyerang akan meluncurkan serangan DDOS sebagai pilihan terakhir. Oleh sebab itu analisis ini bertujuan untuk mengetahui cara kerja suatu serangan DDOS dalam suatu keamanan jaringan komputer. Dan bisa mengetahui titik lemah dari suatu jaringan sehingga bisa merancang dengan aman. Untuk analisis tersebut menggunakan *Packet Tracer* yang bisa dianalisis dengan berbagai cara serangan dan mengambil sumber serangan dengan pengumpulan data dan suatu masalah atau peristiwa yang bisa dianalisis.

***Intrusion Detection System* (IDS)**

Intrusion Detection System (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan (Akhmad, 2013: 2).

Beberapa alasan untuk memperoleh dan menggunakan IDS (*Intrusion Detection System*) (Ariyus, 2007: 31), diantaranya adalah:

1. Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang-orang yang tidak bertanggung jawab dan hukuman yang diberikan atas kegiatan tersebut.
2. Mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem umum pakai seperti *firewall*, sehingga banyak menyebabkan adanya begitu banyak lubang keamanan, seperti:
   a. Banyak dari *legacy* sistem, sistem operasi tidak *patch* maupun *update.*
   b. *Patch* tidak diperhatikan dengan baik, sehingga menimbulkan masalah baru dalam hal keamanan.
   c. *User* yang tidak memahami sistem, sehingga jaringan dan protokol yang mereka gunakan memiliki lubang keamanan.
   d. *User* dan *administrator* membuat kesalahan dalam konfigurasi dan dalam menggunakan sistem.
3. Mendeteksi serangan awal, penyerang akan menyerang suatu sistem yang biasanya melakukan langkah-langkah awal yang mudah diketahui yaitu dengan melakukan penyelidikan atau menguji sistem jaringan yang akan menjadi target, untuk mendapatkan titik-titik dimana mereka akan masuk.
4. Mengamankan *file* yang keluar dari jaringan.
5. Sebagai pengendali untuk rancangan keamanan dan *administrator*, terutama bagi perusahaan yang pesat.
6. Menyediakan informasi yang akurat terhadap gangguan secara langsung, meningkatkan diagnosis, *recovery*, dan mengoreksi faktor-faktor penyebab serangan.

Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara *real time traffic* dan *logging* ke dalam *database* serta mampu mengidentifikasi berbagai serangan yang berasal dari

luar jaringan (Ariyus, 2007:145). Program *snort* dapat dioperasikan dengan tiga mode:

1. *paket sniffer*
   Membaca paket-paket dari jaringan dan memperlihatkan bentuk aliran tak terputus pada konsol (layar). Jika hanya ingin melihat paket-paket *header* dari TCP/IP pada layar cobalah gunakan perintah:
   ```
   ./snort -v
   ```
2. *paket logger*
   Mencatat *log* dari paket-paket ke dalam *disk*. Jika ingin menyimpan catatan paket-paket ke dalam *disk*, maka perlu mencantumkan direktori *logging*, yaitu dimana data *log* disimpan padanya. Melalui perintah berikut *Snort* akan secara otomatis berjalan pada mode pencatatan paket:
   ```
   ./snort –dev –l ./log
   ```
3. NIDS (*Network Intrusion Detection System*)
   Pada mode ini *snort* akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk mengaktifkan *mode* sistem deteksi penyusup jaringan NIDS (*Network Intrusion Detection System*) gunakan perintah berikut:
   ```
   ./snort –dev –l ./log –h 192.168.1.0/24 –c
   snort.conf
   ```

Snort memiliki komponen yang bekerja saling berhubungan satu dengan yang lainnya seperti berikut ini (Ariyus, 2007:146):

1. *Decoder*: sesuai dengan paket yang di-*capture* dalam bentuk struktur data dan melakukan identifikasi protokol, *decode* IP dan kemudian TCP atau UDP tergantung informasi yang dibutuhkan, seperti *port number*, dan IP *address. Snort* akan memberikan peringatan jika menemukan paket yang cacat.
2. *Preprocessors*: suatu saringan yang mengidentifikasi berbagai hal yang harus diperiksa seperti *Detection Engine. Preprocessors* berfungsi mengambil paket yang berpotensi membahayakan, kemudian dikirim ke *detection engine* untuk dikenali polanya.
3. *Rules File*: merupakan suatu *file* teks yang berisi daftar aturan yang sintaksnya sudah diketahui. Sintaks ini meliputi protokol, *address*, *output plug-ins* dah hal-hal yang berhubungan dengan berbagai hal.
4. *Detection Engine*: menggunakan *detection plug-ins*, jika ditemukan paket yang cocok maka *snort* akan menginisialisasi paket tersebut sebagai suatu serangan.
5. *Output Plug-ins*: suatu modul yang mengatur format dari keluaran untuk *alert* dan *file logs* yang bisa diakses dengan berbagai cara, seperti *console, extern files, database,* dan sebagainya.

WinPcap

WinPcap adalah *driver* untuk penangkap paket-paket yang hilir-mudik dalam jaringan. Secara fungsional artinya *WinPcap* menangkap paket-paket dari kabel jaringan dan melemparnya ke program *Snort. WinPcap* mungkin dapat diserupakan dengan libpcap versi *Windows*, yang digunakan untuk menjalankan *Snort* dalam Linux atau UNIX (Rafiudin, 2010: 6). *Driver WinPcap* melakukan fungsi-fungsi berikut untuk *snort*:

1. Menangkap daftar *adapter* jaringan yang beroperasi dan sekaligus mengambil informasi tentang *adapter* tersebut.
2. Mengawasi paket-paket menggunakan salah satu *adapter* yang dipilih.
3. Menyimpan paket-paket ke dalam *hard-drive* (atau lebih penting lagi, meneruskannya ke program *snort*).

PfSense

PfSense adalah *open source firewall* atau *router software* distribusi komputer berbasis *FreeBSD* ini dipasang pada komputer fisik atau mesin *virtual* untuk membuat *firewall* atau *router* khusus untuk jaringan ini dapat dikonfigurasi dan ditingkatkan melalui antarmuka berbasis *web*, dan tidak memerlukan pengetahuan tentang sistem *FreeBSD* yang mendasari untuk dikelola. *PfSense* biasanya digunakan sebagai *firewall perimeter*, *router*, titik akses nirkabel, *server* DHCP, *server* DNS dan sebagai VPN titik akhir *PfSense* mendukung pemasangan paket pihak ketiga seperti *Snort* atau *Squid* melalui *Package Manager*-nya.

VirtualBox

Oracle VM VirtualBox atau sering disebut dengan *VirtualBox* merupakan salah satu produk perangkat lunak yang sekarang dikembangkan oleh *Oracle*. Aplikasi ini pertama kali dikembangkan oleh perusahaan Jerman, *Innotek GmbH*. Februari 2008, *Innotek GmbH* diakusisi oleh *Sun Microsystems. Sun Microsystem* kemudian juga diakuisisi oleh *Oracle*.

VirtualBox berfungsi untuk melakukan virtualisasi sistem operasi. *VirtualBox* juga dapat digunakan untuk membuat virtualisasi jaringan komputer sederhana. Penggunaan *VirtualBox* ditargetkan untuk *Server*, *desktop* dan penggunaan *embedded*. Berdasarkan jenis VMM yang ada, *Virtualbox* merupakan jenis *hypervisor type* 2.

Oracle VM VirtualBox adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama. Sebagai contoh, jika seseorang mempunyai sistem operasi *Microsoft Windows* yang terpasang di komputernya, maka yang bersangkutan dapat pula menjalankan sistem operasi lain yang diinginkan di dalam sistem operasi *Microsoft Windows* tersebut. Fungsi ini sangat penting jika seseorang ingin melakukan ujicoba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada.

Fungsi-fungsi *Virtualbox*

1. Mencoba *Operation System* apapun.
   Virtualbox dapat memainkan semua sistem operasi baik itu menggunakan *Windows*, *Linux* atau turunan *Linux* lainnya. *Virtualbox* juga dapat dipergunakan untuk menguji coba OS baru.
2. Sebagai media untuk membuat simulasi jaringan.
   Di dalam *Virtualbox* dapat membuat banyak mesin *virtual* dan memainkannya sekaligus. Dapat menggabungkan semua mesin yang aktif tadi dalam satu jaringan. Seolah-olah mempunyai banyak komputer yang terkoneksi.
3. Sebagai komputer yang fleksibel dan dapat dipindah-pindahkan.

Misalnya saat membuat sebuah *server* antivirus dan *server* absensi sekaligus untuk keperluan kantor dalam bentuk *virtual* di satu komputer. *Server* antivirus dan absensi dapat dipindahkan ke komputer lain dengan memindahkan mesin *virtual* ke komputer lain jika sewaktu waktu komputer utamanya rusak. Biasanya *format file virtualbox* berekstensi .VDI. maka tinggal *copy paste* format .VDInya saja ke komputer lain.

Jenis Serangan

Beberapa jenis serangan pada jaringan komputer yaitu sebagai berikut:

1. *Ping of Death*
   Jenis serangan pada komputer yang melibatkan pengiriman *ping* yang salah atau berbahaya ke komputer target. Sebuah *ping* biasanya berukuran 56 *byte* (atau 84 *bytes* ketika *header* IP dianggap). Dalam sejarahnya, banyak sistem komputer tidak bisa menangani paket *ping* lebih besar daripada ukuran maksimum paket IP, yaitu 65.535 *byte*. Mengirim *ping* dalam ukuran ini (65.535 *byte*) bisa mengakibatkan kerusakan (*crash*) pada komputer target. Secara tradisional, sangat mudah untuk mengeksploitasi *bug* ini. Secara umum, mengirimkan paket 65.536 *byte ping* adalah *illegal* menurut protokol jaringan, tetapi sebuah paket semacam ini dapat dikirim jika paket tersebut sudah terpecah-pecah. Ketika komputer target menyusun paket yang sudah terpecah-pecah tersebut, sebuah *buffer overflow* mungkin dapat terjadi seperti *crash*.
2. *Nmap* (*Port Scan*)
   Nmap (*Network Mapper*) adalah sebuah aplikasi atau *tool* yang berfungsi untuk melakukan *port scanning*. *Nmap* dibuat oleh Gordon Lyon, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk meng-*audit* jaringan yang ada. Dengan menggunakan *tool* ini, dapat melihat *host* yang aktif, *port* yang terbuka, sistem operasi yang digunakan, dan fitur-fitur *scanning* lainnya.
3. *Denial of Service* (DOS)
   Merupakan sebuah jenis serangan terhadap sebuah komputer atau *server* di dalam jaringan internet. DOS ini bekerja dengan cara menghabiskan *resource* yang dimiliki oleh komputer tersebut sampai akhirnya komputer tersebut tidak dapat menjalankan fungsinya dengan benar. DOS ini akan menyerang dengan cara mencegah seorang pengguna untuk melakukan akses terhadap sistem atau jaringan yang dituju. Ada beberapa cara yang dilakukan oleh DOS untuk melakukan serangan tersebut, yaitu:
   a. Membanjiri *traffic* atau lalu lintas jaringan dengan banyaknya data-data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Biasanya teknik ini disebut sebagai *traffic flooding*.
   b. Membanjiri jaringan dengan cara me-*request* sebanyak-banyaknya terhadap sebuah layanan jaringan yang disediakan oleh sebuah *client* sehingga *request* yang datang dari para pengguna terdaftar tidak dapat dilayani aleh layanan tersebut. Biasanya teknik ini disebut sebagai *request flooding*.
4. *Trojan Horse*
   Merupakan salah satu jenis *Malicious software* atau *malware* yang dapat merusak sebuah sistem. *Trojan* ini dapat digunakan untuk memperoleh informasi dari target seperti *password*, *system log* dan lain-lain, dan dapat memperoleh hak akses dari target. *Trojan* merupakan *software* yang berbeda dengan *virus* atau *worm* karena *trojan* ini bersifat *stealth* dalam beroperasi dan seolah-olah seperti program biasa yang tidak mencurigakan dan *trojan* juga bisa dikendalikan dari komputer lain (*attacker*). Berikut jenis-jenis *Trojan*, yaitu:
   a. Pencuri *Password*: jenis *trojan* ini dapat mencuri *password* yang disimpan didalam sistem dengan cara membuat tampilan seolah-olah tampilan *login* dengan menunggu *host* memasukan *password*-nya pada saat *login* kemudian *password* tersebut akan dikirimkan ke *attacker*.
   b. *Keylogger*: jenis *Trojan* akan merekam semua yang diketikan oleh *host* dan mengirimkanya ke *attacker*.

   RAT (*Remote Administration Tools*): jenis *trojan* ini mampu mengambil alih kontrol secara penuh terhadap sistem dan dapat melakukan apapun yang *attacker* mau dari jarak jauh seperti mem-*format harddisk*, meng-*edit* dan menghapus data.

III. METODE PENELITIAN

Analisis Permasalahan Sistem Jaringan

Permasalahan pada sistem jaringan di SMAN 1 Cikeusal yaitu masih kurangnya sistem keamanan jaringan dan pengawasan terhadap penyalahgunaan jaringan yang hanya menggunakan *router mikrotik* bawaan sebagai *firewall*. Banyak penyimpanan data-data pada sekolah dan manajemen jaringan yang tidak terkontrol dengan baik menjadi permasalahan yang harus diperbaiki serta penyalahgunaan jaringan seperti

akses sosial media yang sering diakses oleh siswa-siswi pada saat jam pelajaran berlangsung.

Alternatif Pemecahan Masalah

Dengan adanya sebuah sistem keamanan *Intrusion Detection System* (IDS) *Snort* dan penamabahan *PfSense (Router OS)* sebagai tindakan lanjut dari proses *snort* yang dihasilkan *alert* tersebut. Sehingga peningkatan sistem keamanan jaringan dan komputer akan lebih meningkat dari sebelumnya seperti adanya serangan ataupun penyalahgunaan jaringan yaitu mengakses sosial media.

Spesifikasi *Hardware* dan *Software*

Spesifikasi *hardware* dan *software* yang digunakan yaitu:

1. *Hardware*

   Pada pemasangan *Snort*, *Hardware* yang digunakan adalah sebagai berikut:

Tabel 1. Analisis *Hardware* Komputer

Hardware	Keterangan
Processor	Intel Core i5 3.2 GHz
Memory	4 GB DDR3
Harddisk	1TB

Sumber: Dokumen Pribadi

2. *Software*

   Software yang digunakan pada komputer yang terpasang *Snort* yaitu:

Tabel 2. Analisis *Software* Komputer

Software	Keterangan
Sistem Operasi	*Windows 7 Ultimate* 64-bit
Snort	Aplikasi atau *tool security*
PfSense	*Router OS*

Sumber: Dokumen Pribadi

Rancangan Aplikasi

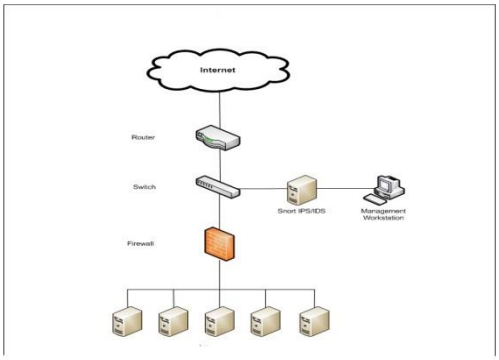
Perancangan sistem yang akan digunakan untuk merancang suatu sistem yang dapat mendeteksi adanya penyusup ataupun serangan yaitu *Intrusion Detection System*, yang sebelumnya membutuhkan *tools* atau komponen yang diperlukan untuk membangun sistem tersebut yang nantinya akan bekerja sama untuk mendapatkan hasil yang maksimal.

1. *Snort*
2. *WinPcap*
3. *PfSense*
4. *VirtualBox*

Manajemen Jaringan Usulan

IDS merupakan suatu sistem yang memiliki kemampuan untuk menganalisis data secara *realtime* dalam mendeteksi, mencatat (*log*) dan menghentikan penyalahgunaan dan penyerangan. IDS merupakan *security tools* yang dapat digunakan untuk menghadapi aktivitas *hackers.* IDS ini mampu memberikan peringatan kepada *administrator* apabila terjadi suatu serangan atau penyalahgunaan di dalam jaringan, bahkan peringatan itu dapat pula menunjukkan alamat IP dari sebuah sistem penyerang.

Topologi Jaringan Usulan



Sumber: Dokumen Pribadi

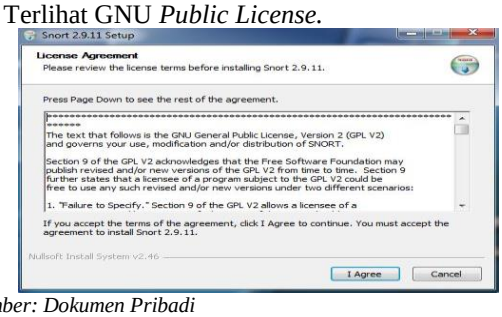
Gambar 1. Topologi Jaringan Usulan

Instalasi *Snort*

Snort menyediakan paket instalasi yang cocok untuk *versi Windows* yang dapat di-*download* dari *link*: http://www.snort.org/dl/binaries/win32 berikut ini langkah-langkah untuk menginstal *snort*:

1. Klik ganda *file* instalasi tersebut untuk mulai menginstal.

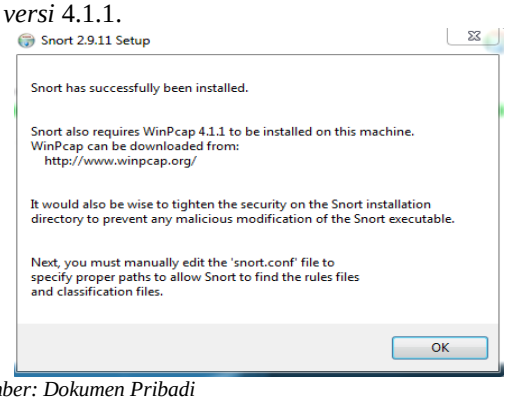
   Terlihat GNU *Public License.*



Sumber: Dokumen Pribadi

Gambar 2. GNU *Public License*

2. Langkah selanjutnya mengklik tombol "*I Agree*" dan "*next*" sampai instalasi selesai dan klik tombol OK. Maka *snort* sudah berhasil terpasang dan meminta untuk menginstal *WinPcap* minimum *versi* 4.1.1.



Sumber: Dokumen Pribadi

Gambar 3. *Request Installed WinPcap*

Instalasi *WinPcap*

Instalasi dan konfigurasi *WinPcap* hampir tidak memerlukan intervensi, yaitu:

1. *Download file* instalasi WinPcap terkini dari http://www.winpcap.org/.

2. Klik ganda instalasi tersebut dan ikuti petunjuk instalasi yang diberikan.

WinPcap menginstal dirinya sendiri ke lokasi yang telah ditetapkan secara defalut. *Snort* akan memanggil *WinPcap* secara langsung pada semua fungsi untuk menangkap dan menganalisis paket-paket jaringan. Ini artinya jika *driver* tersebut tidak terinstal dengan benar maka *snort* tidak akan berfungsi.

Konfigurasi *Snort*

Untuk mengkonfigurasi dengan membuka *file* `snort.conf` yang terdapat pada *Folder* `C:\Snort\etc` kemudian *edit* dengan menggunakan *text editor*, akan tetapi lebih disarankan menggunakan *Notepad++*.

Konfigurasi *Rule Snort*

Selanjutnya sebelum menjalan *snort* tersebut, maka membutuhkan beberapa langkah lagi yaitu dengan mengkonfigurasikan *rules snort* agar *snort* dapat bekerja dengan baik.

Rules snort tersebut dapat diperoleh pada http://www.snort.org/snort-rules/?#rules, tetapi sebelum men-*download rules snort* tersebut maka terlebih dahulu harus melakukan registrasi terhadap situs *snort* yaitu http://www.snort.org.

Setelah berhasil men-*download rules snort* tersebut, langkah selanjutnya meng-*ekstrak snort rules* ke direktori `C:\snort`. Proses akan berhasil ditandai dengan adanya beberapa *rules* berformat `.rules` pada direktori `C:\snort\rules`.

Menjalankan *Snort*

Menjalankan *snort* yaitu dengan menggunakan *Command Prompt* dalam modus *Administrator*. Caranya adalah dengan memilih *icon Command Prompt*, meng-klik kanan dan memilih menu "*Run As Administrator*". Sebelum itu perhatikan *options* yang diberikan oleh *snort*.

IV HASIL DAN PEMBAHASAN

Pengujian Jaringan Awal

Pada pengujian awal yang dilakukan yaitu kepada komputer yang tidak terpasang oleh *snort* dan mencoba menyerang komputer tersebut. Hasil yang diperoleh yaitu:

1. Ketika ada percobaan serangan dan penyalahgunaan jaringan, komputer tidak mengetahui jika seseorang hendak menyerang kepada komputer yang tidak terpasang oleh *snort*.
2. *Snort* yang belum terpasang di komputer membuat tidak bisanya membaca *traffic* lalu lintas jaringan karena untuk melihat *traffic* lalu lintas paket-paket pada jaringan harus terpasang terlebih dahulu *snort* tersebut.

Sumber: Dokumen Pribadi

Gambar 4. Respon Komputer yang Belum Terpasang *Snort*

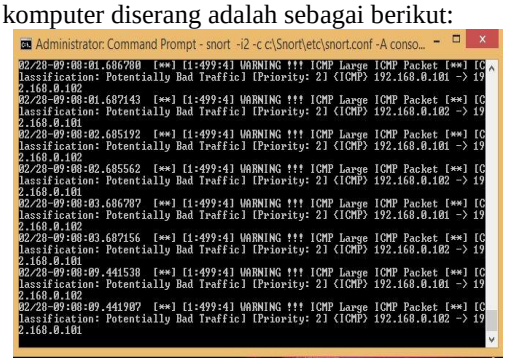
Pengujian Jaringan Akhir

Pada pengujian akhir Komputer akan terpasang sistem *snort*. Sistem *snort* akan dicoba dengan percobaan serangan dan akan menampilkan *alert* sesuai ancamannya dan menampilkan penyalahgunaan jaringan yang terdeteksi.

Tahapan Pengujian

1. *Ping of Death*

   Komputer yang terpasang *Snort* akan dicoba dengan metode penyerangan *ping of death* dari komputer penyerang. Hasil yang terjadi pada saat komputer diserang adalah sebagai berikut:

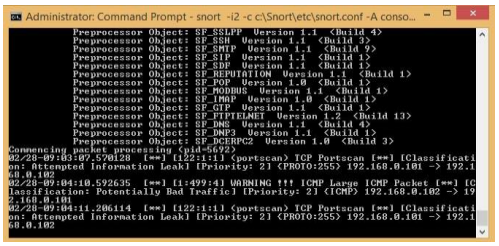


Sumber: Dokumen Pribadi

Gambar 5. Serangan *Ping of Death*

Gambar 5 menunjukkan IP 192.168.0.101 (komputer penyerang) melakukan *ping of death* terhadap IP 192.168.0.102 (komputer yang terpasang *snort*) dengan peringatan "*WARNING !!! ICMP Large ICMP Packet*".

2. *Port Scan*



Sumber: Dokumen Pribadi

Gambar 6. Serangan *Port Scan*

Gambar 6 menunjukkan IP 192.168.0.101 (komputer penyerang) melakukan *port scan* terhadap IP 192.168.0.102 (komputer yang terpasang *snort*) dan menghasilkan *alert* peringatan "<*portscan*> TCP *port scan*".

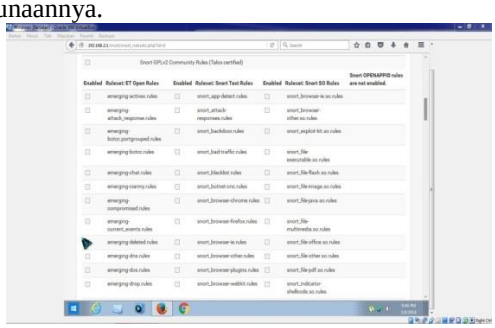
3. *PfSense*

Buka *PfSense* pada dan muncul tampilan seperti ini, maka untuk *login* ke halaman *PfSense* dengan memasukkan IP LAN pada *browser*:

Sumber: Dokumen Pribadi

Gambar 7. Tampilan Awal *PfSense* Berjalan

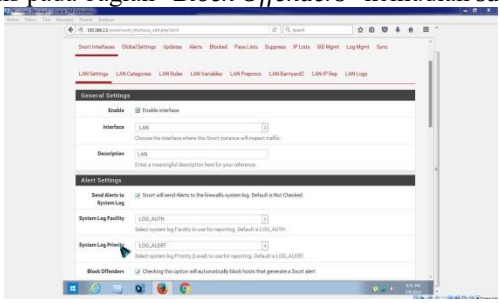
Pemilihan *Rules* yang bisa diaktifkan sesuai kegunaannya.



Sumber: Dokumen Pribadi

Gambar 8. Mengaktifkan *Rule* yang akan Digunakan

Mengatur *General Setting* untuk *block* otomatis ceklis pada bagian "*Block Offenders*" kemudian *save*.



Sumber: Dokumen Pribadi

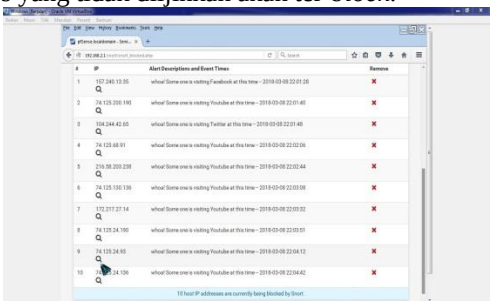
Gambar 9. *Setting Alert* yang Ter-*block* secara Otomatis

Hasil setelah seseorang mencoba mengakses sebuah akses yang tidak diijinkan.

Sumber: Dokumen Pribadi

Gambar 10. *Alert* yang Dihasilkan

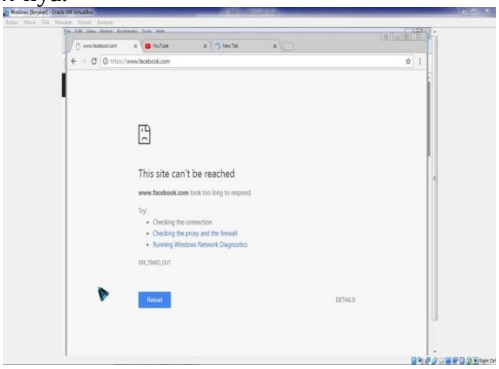
Secara otomatis pengguna yang mengakses suatu akses yang tidak diijinkan akan ter-*block*.



Sumber: Dokumen Pribadi

Gambar 11. IP yang Ter-*block*

Tampilan setelah *alert* menampilkan ada seseorang yang mengakses media sosial dan langsung mem-*block*-nya.



Sumber: Dokumen Pribadi

Gambar 12. Media yang tidak Bisa Diakses karena Ter-*block*

Analisis

Hasil yang didapat pada pengujian *snort* bahwa *alert* yang dihasilkan oleh *snort log* dapat membaca paket-paket yang lewat sesuai kondisi yang terjadi pada jaringan.

Komputer yang tidak terpasang *snort* tidak bisa mengetahui apa yang seadang terjadi pada komputernya seperti serangan dan penyalahgunaan jaringan seperti mengakses sosial media.

Berdasarkan percobaan serangan dengan komputer yang terpasang *snort* dapat mengetahui apa yang sedang terjadi yang dihasilkan pada *alert*. Pada *PfSense* menampilkan *alert* jika ada seseorang yang mencoba menyalah gunakan jaringan seperti mengakses sosial media *facebook*, *youtube*, *twitter* dan lain-lain bisa menindak lanjuti dengan mem-*block* secara otomatis.

Log yang dihasilkan dapat membaca suatu serangan dan penyalahgunaan jaringan sesuai dengan metode pengujiannya dengan menyeting bagian *rule* dari *snort*.

Snort tidak bisa menindak lanjuti *alert* yang terdeteksi sebagai serangan atau penyalahgunaan jaringan karena sifatnya hanya mendeteksi maka penggunaan *Pfsense* adalah sebagai penindak lanjutan dari *alert* yang dihasilkan sehingga bisa dicegah dengan cara mem-*block*. Meski *PfSense* adalah *Router OS* tetapi ada penggunaan *Snort* di dalamnya.

V PENUTUP

Kesimpulan

Berdasarkan penelitian yang telah dilakukan, ada beberapa hal yang penulis simpulkan, yaitu:

1. Pada metode penyerangan IDS *snort* mampu mendeteksi adanya serangan seperti *Ping Of Death* dan *Port Scan.*
2. *Log* yang dihasilkan dapat membaca suatu serangan dan penyalahgunaan jaringan sesuai dengan metode pengujiannya dengan menyeting bagian *rule* dari *snort*.
3. *Snort* tidak bisa menindak lanjuti *alert* yang terdeteksi sebagai serangan atau penyalahgunaan jaringan karena sifatnya hanya mendeteksi.
4. Penggunaan *Pfsense* adalah sebagai penindak lanjutan dari *alert* yang dihasilkan sehingga bisa dicegah dengan cara mem-*block* seperti penyalahgunaan jaringan dengan mengakses sosial media seperti *facebook, youtube, twitter* dan lain lain.

Saran

Berdasarkan uraiaan dari kesimpulan, maka kelebihan dan kekurangan di atas dapat menjadi pelajaran serta referensi untuk ke depannya. Saran-saran yang dapat dipertimbangkan untuk ke depan antara lain:

1. Dalam membangun sistem keamanan jaringan perlu diperhatikan dari sisi penempatan sistem *snort*-nya, karena sangat berpengaruh terhadap jaringan yang terhubung satu dengan yang lainnya.
2. Dilakukannya pengujian gangguan serangan terhadap jaringan yang berbeda, tidak hanya pada dalam satu jaringan saja.
3. Mempelajari lebih dalam dari fungsi-fungsi *rules snort.*

DAFTAR PUSTAKA

Angela, O. dkk. (2007). *Wireshark & Ethereal network protocol analyzer toolki.* Canada: Syngress.

Ariyus, D. (2007). *Intrusion Detection System*. Yogyakarta: Andi.

Becky, P. dan Angela, O. (2008). *Nmap in the Enterprise: Your Guide to Network Scanning*. United State of America: Syngress.

Caswell, B. Dkk. (2004). *Snort 2.1 Intrusion Detection Second Edition*. United States of America: Syngress.

Ferianto, S. (2013). *Jenis-jenis serangan jaringan komputer*. [Online]. Tersedia: http://www.tutorialcarakomputer.com/2014/03/jenis-jenis-serangan-pada-jaringan-komputer.html [02 November 2017].

Gobel. Dkk. (2014). "Analisa dan Pengembangan Sistem Peringatan Keamanan Jaringan Komputer Menggunakan SMS Gateway dan Paket Filter." *Pengembangan Terhadap Sistem Keamanan.* Vol.1. No.(2). 382-388

Gufron, R. (2013). *Mengenal Aplikasi Virtualisasi Oracle VM VirtualBox*. [Online]. Tersedia: http://dosen.gufron.com/artikel/mengenal-aplikasi-virtualisasi-oracle-vm-virtualbo/10/ [24 Februari 2018].

Hakim, A. dkk. (2014). "Rancang Bangun GUI Intrusion Prevention System (IPS) Suricata." *Pengembangan dan Pemanfaatan Riset IoT (Internet of Things) untuk Bidang Pendidikan dan Industri*. Vol.1. No.(1). 268-275

Hermawan, R. (2011). "Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denial of Service (DDOS)." *Analisis Konsep dan Cara Kerja Serangan.* Vol.5 No.(1). 1-14

Purbo. dkk. (2000). *Keamanan jaringan internet.* Jakarta: Elex Media Komputindo, Penerbit Kelompok Gramedia.

Rafiudin, R. (2007). *Panduan Menjadi Administrator Unix*. Yogyakarta: Penerbit Andi.

Rafiudin, R. (2010). *Mengganyang Hacker dengan Snort*. Yogyakarta: Penerbit Andi.

Riadi, I. (2011). "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik." *Optimalisasi Keamanan Jaringan*. Vol.1 No.(1). 1-5

Santoso. dkk. (2011). "Manajemen Keamanan Jaringan Informasi Menggunakan IDS/IPS Strataguard Studi Kasus STIMK Amikom Yogyakarta." *Manajemen Keamanan Jaringan dengan Berbagai Metode*. Vol.12 No.(1). 9-22

Sumardi. dan Triyono, R. A. (2012). "Rancang Bangun Sistem Keamanan Jaringan dengan Metode Blocking Port pada Sekolah Menengah Kejuruan Karya Nugraha Boyolali." *Meningkatkan Performance Jaringan Internet.* Vol.2 No.(1). 16-21

Yusuf, F. (2017). *Mengenal Berbagai Jenis Serangan pada Jaringan Komputer*. [Online]. Tersedia: http://netsec.id/jenis-serangan-jaringan-komputer/ [24 Februari 2018]