Monitoring Keamanan Jaringan Komputer Menggunakan Network Intrussion Detection System (NIDS)

Ery Setiyawan Jullev Atmaji[1], Bekti Maryuni Susanto[2]

[1,2]*Jurusan Teknologi Informasi, Politeknik Negeri Jember*
Jl. Mastrip Kotak Pos 164 Jember

[1]setiyawanjullev@gmail.com

[2]bekti.polije@gmail.com

Abstract

Instruksi Teknologi informasi dewasa ini semakin berkembang dan pertumbuhan yang signifikan. Contohnya mulai dari sistem informasi, *mobile phone, smart home,* dan yang terbaru adalah *virtual reality.* Tidak hanya itu, untuk mendukung keamanan jaringan pun dituntut untuk lebih berkembang dalam melindungi data yang ada pada jaringan. Keamanan jaringan merupakan segala aktifitas pengamanan suatu jaringan dengan bertujuan menjaga *privacy, integrity, availability, authentication, access control* dan *safety* terhadap suatu serangan. Keamanan jaringan harus mampu mencegah dan menghentikan berbagai potensi serangan agar tidak memasuki dan menyebar pada sistem jaringan. Serangan atau *Intrusion* dapat diartikan sebagai aktivitas tidak sah atau tidak diinginkan yang mengganggu privasi, integritas dan atau ketersediaan dari informasi yang terdapat di sebuah sistem. Oleh karena itu dibutuhkan suatu sistem keamanan jaringan yang mempunyai tampilan antar muka yang mudah dipahami oleh administrator sehingga memungkinkan administrator untuk mengkases sistem walaupun terjadi malfungsi jaringan serta agar mempercepat prosess penanggulangan gangguan dan pemulihan sistem. Penelitian ini menerapkan salah satu Network Intrussion Detection System yaitu SNORT IDS yang diintegrasikan dengan BASE. Hasil monitoring SNORT ditampilkan dalam bentuk tampilan website menggunakan BASE.

Keywords— Network Intrussion Detection System, SNORT IDS, BASE.

I. PENDAHULUAN

Teknologi informasi dewasa ini semakin berkembang dan pertumbuhan yang signifikan. Contohnya mulai dari sistem informasi, *mobile phone*, *smart home*, dan yang terbaru adalah *virtual reality*. Tidak hanya itu, untuk mendukung keamanan jaringan pun dituntut untuk lebih berkembang dalam melindungi data yang ada pada jaringan. Keamanan jaringan merupakan segala aktifitas pengamanan suatu jaringan dengan bertujuan menjaga *privacy*, *integrity*, *availability*, *authentication*, *access control* dan *safety* terhadap suatu serangan. Keamanan jaringan harus mampu mencegah dan menghentikan berbagai potensi serangan agar tidak memasuki dan menyebar pada sistem jaringan. Serangan atau *Intrusion* dapat diartikan sebagai aktivitas tidak sah atau tidak diinginkan yang mengganggu privasi, integritas dan atau ketersediaan dari informasi yang terdapat di sebuah sistem.

Sistem pendeteksi jaringan yang ada pada saat ini umumnya mampu mendeteksi berbagai jenis serangan namun tidak cukup mampu untuk melakukan tindakan lebih lanjut. Selain itu sistem keamanan pun juga tidak memiliki interaktivitas dengan admin pada saat admin tidak mengadministrasi sistemnya. Selain itu sistem keamanan ini umumnya dilakukan secara manual oleh administrator. Hal ini mengakibatkan integritas sistem bergantung pada administrator dalam merespon setiap gangguan yang ada.

Oleh karena itu dibutuhkan suatu sistem keamanan jaringan yang mempunyai tampilan antar muka yang mudah dipahami oleh administrator sehingga memungkinkan administrator untuk mengkases sistem walaupun terjadi malfungsi jaringan serta agar mempercepat prosess penanggulangan gangguan dan pemulihan sistem.

Metode penelitian yang digunakan adalah metode penelitian eksperimen. Pada penelitian ini network instrussion detection system (NIDS) yang digunakn adalah Snort IDS. Selanjutnya diukur tingkat akurasi Snort dalam mendeteksi srangan pada jaringan komputer.

II. TINJAUAN PUSTAKA

IDS (Intrusion Detection System) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi

aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. *IDS* dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem jaringan, melakukan analisis dan mencari bukti dari percobaan penyusupan (intrusi). *IDS* mempunyai beberapa komponen yaitu :

A. Sensor yang dapat mengenali adanya *security events.*
B. *Console* yang dapat memonitor *event* dan *alerts* dan mengontrol sensor.
C. *Centarl Engine* yang berguna untuk menyimpan *events logged* yang dilakukan oleh sensor kedalam *database* dan menggunakan aturan-aturan keamanan yang berguna untuk menangani *event* yang terjadi

1.*Jenis-JenisIDS :* Dilihat dari kemampuan mendeteksi serangan atau penyusupan di dalam jaringan, maka *IDS*dibagi menjadi 2 yaitu :

a). Network-based Intrusion Detection System (NIDS), menganilsa semua lalu lintas yang melewati ke sebuah jaringan yang akan mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. Kelemahan *NIDS* adalah rumit untuk diimplementasikan dalam sebuah jaringan yang menggunakan *switch ethernet*, meskipun beberapa *vendor switch ethernet* sekarang telah menerapkan fungsi *IDS* di dalam *switch* buatannya untuk memonitor *port* atau koneksi

b). Host Intrution Detection System (HIDS): IDS jenis ini berjalan pada *host* yang berdiri sendiri atau perlengkapan dalam sebuah jaringan. Sebuah *HIDS* melakukan pengawasan terhadap paket-paket yang berasal dari dalam maupun dari luar hanya pada satu alat saja dan kemudian memberi peringatan kepada *user* atau adminitrator jaringan akan adanya kegiatan-kegiatan yang mencurigakan yang terdeksi oleh *HIDS.*

c). Signature Based : *IDS* yang berbasis pada *signature* akan melakukan pengawasan terhadap paket-paket dalam jaringan dan melakukan pembandingan terhadap paket-paket tersebut dengan basis data *signature* yang dimilki oleh sistem *IDS* ini atau atribut yang dimilki oleh percobaan serangan yang pernah diketahui. Cara ini hampir sama dengan cara kerja aplikasi antivirus dalam melakukan deteksi terhadap *malware.* Intinya akan terjadi keterlambatan antara terdeteksinya sebuah serangan di *internet* dengan *signature* yang digunakan untuk melakukan deteksi yang di implementasikan didlam basis data *IDS* yang digunakan. Jadi bisa saja basis data *signature* yang digunakan dalam sistem *IDS* ini tidak mampu mendeteksi adanya sebuah percobaan serangan terhadap jaringan karena informasi jenis serangan ini tidak terdapat dalam basis data *signature* sistem *IDS.* Selama waktu keterlambatan tersebut sistem *IDS* tidak dapat mendeteksi adanya jenis serangan baru.

d). Anomaly Based

IDS jenis ini akan mengawasi *traffic* dalam jaringan dan melakukan perbandingan *traffic* yang terjadi dengan rata-rata *traffic* yang ada (stabil). Sistem akan melakukan indentikasi apa yang dimaksud dengan jaringan "normal" dalam jaringan tersebut, berapa banyak *bandwidth* yang biasanya digunakan di jaringan tersebut, *protocol* apa yang digunakan, *port-port* dan alat-alat apa saja yang biasanya saling berhubungan satu sama lain didalam jaringan tersebut, dan memberi peringatan kepada administrator ketika dideteksi ada yang tidak normal, atau secara signifikan berbeda dari kebiasaan yang ada.

e). Passive IDS

IDS jenis ini hanya berfungsi sebagai pendeteksi dan pemberi peringatan. Ketika *traffic* yang mencurigakan atau membahayakan terdeteksi oleh *IDS* maka *IDS* akan membangkitkan sistem pemberi peringatan yang dimiliki dan dikirimkan ke adminsistrator atau *user* dan selanjutnya akan ditindak lanjuti oleh administrator.

f) Reactive IDS

IDS jenis ini tidak hanya melakukan deteksi terhadap *traffic* yang mencurigakan dan membahayakan kemudian memberi peringantan kepada administrator tetapi juga mengambil tidakan pro aktif untuk merespon terhadap serangan yang ada. Biasanya dengan melakukan pemblokiran terhadap *traffic* jaringan selanjutnya dari *ip address* sumber atau *user* jika *ip address* sumber atau *user* tersebut mencoba untuk melakukan serangan lagi terhadap sistem jaringan di waktu selanjutnya.

2 Fungsi *IDS*

Beberapa alasan untuk memperoleh dan menggunakan *IDS* (*Ariyus*, 2007) , diantaranya :

a). Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang-orang yang tidak bertanggung jawab.
b). Mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem umum pakai, seperti *firewall.* Sehingga banyak menyebabkan adanya lubang kemanan, seperti :
   1). Banyak dari *legacy system,* sistem operasi tidak *pacth* maupun *update. Pacth* tidak diperhatikan dengan baik, sehingga menimbulkan masalah baru dalam hal keamanan.
   2). User yang tidak memahami sistem, sehingga jaringan dan protokol yang meraka gunakan memiliki celah dari keamanannya.
   3). User dan administrator membuat kesalahan dalam konfigurasi dan dalam menggunakan sisem
c). Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang-orang yang tidak bertanggung jawab.
d). Mengamankan *file* yang keluar dari jaringan sebagai pengendali untuk rancangan keamanan dan administrator, terutama bagi perusahaan yang besar.

3. Komponen Pada *Snort*

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

a). *Rule Snort*. Merupakan database yang berisi pola-pola serangan berupa signature jenis-jenis serangan. *Rule Snort* IDS ini, harus di *update* secara rutin agar, ketika ada suatu teknik serangan yang baru *Snort* bisa mendeteksi karena jenis atau pola serangan tersebut sudah ada pada *rule snort.*

b). *Snort Engine*. Merupakan program yang berjalan sebagai proses yang selalu bekerja untuk membaca paket data dan kemudian membandingkannya dengan rule Snort.

c). *Alert*, merupakan catatan serangan pada deteksi penyusupan, jika snort engine menyatakan paket data yang lewat sebagai serangan, maka snort engine akan mengirimkan alert berupa log file. Untuk kebutuhan analisa, alert dapat disimpan di dalam database.

d). *Preprocessors*, merupakan suatu saringan yang mengidentifikasi berbagai hal yang harus diperiksa seperti *Snort Engine*. *Preprocessors* berfungsi mengambil paket yang berpotensi membahayakan, kemudian dikirim ke *Snort engine* untuk dikenali polanya

e). *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.

4. *Rule Snort*

Snort Rules merupakan database yang berisi pola-pola serangan berupa *signature* jenisjenis serangan. *Snort Rules* IDS ini, harus *diupdate* secara rutin agar ketika ada suatu teknik serangan yang baru, serangan tersebut dapat terdeteksi. Sebagai contoh *rule* pada *Snort* sebagai berikut : alert tcp $EXTERNAL NET alert tcp $EXTERNAL NET any -> $HTTP SERVERS $HTTP PORTS (msg:"WEB-IIS unicode directory traversal attempt"; flow:to server, established; content:¨/..%c0%af../"; nocase; classtype:web-application-attack; reference:cve, CVE-2000-0884; sid:981; rev:6;)

Rule di atas terdiri dari 2 bagian: *header* dan *option*. Bagian ”alert tcp $EXTERNAL NET any - $HTTP SERVERS $HTTP PORTS” adalah *header* dan selebihnya merupakan option. Dari *rule-rule* seperti di ataslah IDS *Snort* menghukumi apakah sebuah paket data dianggap sebagai penyusupan / serangan atau bukan, paket data dibandingkan dengan *rule* IDS, jika terdapat dalam *rule*, maka paket data tersebut dianggap sebagai penyusupan / serangan dan demikian juga sebaliknya jika tidak ada dalam *rule* maka dianggap bukan penyusupan / serangan. Setelah menginstal *Snort engine* dan *rulesnya*, maka langkah selanjutnya adalah mengkonfigurasi *Snort engine*. *Snort engine* dimodifikasi sesuai kebutuhan dan spesifikasi jaringan yang akan dipindai oleh *Snort*.

Cara kerja *Snort rules* dengan membacabaca *rules* ke dalam struktur atau rantai data *internal*kemudian dicocokkan dengan paket yang ada. Jika paket sesuai dengan *rules* yang ada, tindakanakan diambil, jika tidak paket akan dibuang. Tindakan yang diambil dapat berupa *logging* paket ataumengaktifkan *alert.*

BASE adalah sebuah *interface web* untuk melakukan analisis dari intrusi yang snort telah deteksi pada jaringan. (Orebaugh, 2008:217) *BASE* ditulis oleh Kevin Johnson adalah program analisis sistem jaringan berbasis *PHP* yang mencari dan memproses *database* dari *security event* yang dihasilkan oleh berbagai program monitoring jaringan, *firewall*, atau sensor *IDS*. Berikut ini adalah beberapa kelebihan dari *BASE* yaitu :

a). Program berbasis *web* yang memungkinkan implementasi antar *platform*.
b). *Log - log* yang sulit untuk dibaca akan menjadi mudah untuk dibaca.
c). Data - data dapat dicari sesuai dengan kriteria tertentu.
d). *pen source* yang merupakan perintis antarmuka *GUI* untuk *snort* dan paling banyak digunakan oleh pengguna *IDS*. *BASE* merupakan rekomendasi dari *Snort.org* sendiri.
e). *Multi language,* antarmuka memilki beberapa bahasa selain bahasa Inggris dan layanan peringatan yang *real time.*
f). Dapat diimplementasikan pada *IDS* manapun selain *snort*.

BASE merupakan *PHPBased Analysis Engine*yang berfungsi untuk mencari dan mengolah*databas*e dari *alert network security* yang dibangkitkan oleh perangkat lunak pendeteksi intrusi (*IDS*). Dapat diimplementasikan pada sistem yang mendukung *PHP* seperti *linux*, *BSD*, *Solaris* dan OS lainnya. *BASE* adalah perangkat lunak yang *open - source*. Namun untuk menginstall *BASE* ini dibutuhkan beberapa *software* pendukung yaitu *MySQL*, *PHP*, dan *Apache*.

Berikut ini adalah beberapa Fitur yang ada pada BASE (*Basic Analysis Security Engine*) :

a). Ditulis dalam bahasa *PHP*.
b). Menganalisa *log intrusi*.
c). Mendisplay informasi *database* dalam bentuk web.
d). Mengenerate *graph* dan *alert* berdasarkan *sensor*, waktu *rule* dan *protocol.*
e). Mendisplay *summary log* dari semua *alert* dan *link* untuk *graph.*
f). Dapat diatur berdasarkan kategori grup *alert, false positif* dan *email.*

III. TUJUAN DAN MANFAAT

Tujuanpenelitian ini adalah:

A. Membuat rancangan Netwrok Intrussion Detection System menggunakan Snort IDS.

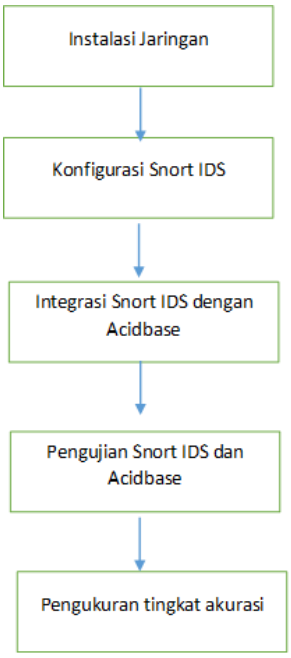
B. Mengintegrasikan Snort IDS dengan Acidbase.
C. Mengukur tingkat akurasi Snort IDS dalam mendeteksi serangan pada jaringan komputer.

Manfaatpenelitian ini adalah:

1. Mendeteksi serangan pada jaringan komputer secara real time.
2. Menjamin terpenuhinya aspek-aspek dalam keamanan jaringan yaitu, confidentiality, integrity dan acountability.
3. Mempermudah administrator dalam mengelola tindakan yang diperlukan untuk menangani permasalahan dalam keamanan jaringan.

IV. METODE PENELITIAN

Penelitian ini adalah penelitian eksperimen dimana pada penelitian dilakukan investigasi mengenai hubungan sebab akibat. Pada penelitian ini terdapat tahapan-tahan penelitian yang akan dilakukan seperti ditunjukkan gambar 1.



Gambar 1. Tahapan penelitian

Penelitian ini dilaksanakan di Laboratorium Arsitektur Jaringan Komputer Politeknik Negeri Jember selama 4 bulan dari bulan September sampai dengan bulan Desember 2016. Objek penelitian yang diamati dalam penelitian ini adalah network intrussion detection system (NIDS) yang terintegrasi dengan acidbase. Variable penelitian yang digunakan pada penelitian ini adalah tingkat akurasi Snort IDS dalam mendeteksi serangan pada jaringan komputer.

V. HASIL DANLUARAN YANG DICAPAI

Penelitian ini menggunakan sistem operasi Linux Ubuntu 14.04 yang terhubung ke dalam sebuah jaringan lokal (client) menggunakan switch. Linux Ubuntu 14.04 ini dipilih karena sifatnya yang open source serta kemudahan dalam melakukan modifikasi maupun konfigurasi paket-paket yang dibutuhkan dalam monitoring keamanan jaringan komputer berbasis network intrussion detection system (NIDS). Software NIDS yang digunakan dalam penelitian ini adalah Snort IDS versi 2.9.8.3. Agar hasil monitoring yang dilakukan oleh NIDS dapat dibaca dengan mudah perlu diinstal aplikasi atau paket untuk menyimpan ke dalam database, yaitu barnyard2. Software database yang digunakan MySql database. Selanjutnya perlu diinstall web server agar data-data yang ada di mysql bisa ditampilkan melalui web bowser. Aplikasi web server yang digunakan adalah apache dan php. Berikut langkah-langkah yang dilakukan pada penelitian ini.

A. Instalasi Jaringan

Jaringan yang digunakan pada penelitian ini adalah jaringan lokal yang terdiri dari 1 komputer server dan 1 komputer client. Komputer server bisa diakses melalui alamat IP Address 192.168.56.130. Sedang komputer client bisa diakses melalui IP Addres 192.168.56.1. Komputer server dan komputer client terhubung melalui sebuah switch.

B. Konfigurasi SNORT IDS

SNORT diinstal pada komputer server yang nantinya berfungsi untuk menangkap paket data yang masuk ke komputer server tersebut. File source code snort dapat diunduh pada website snort.org. Sebelum melakukan instalasi Snort IDS perlu menginstal beberapa software pendukung, yaitu zlibg, liblzma, openssl dan libssl.

Setelah snort berhasil diinstal selanjutnya snort dikonfiurasi agar bisa menangkap paket data yang masuk ke komputer server. Selain itu juga perlu dibuatkan file dan direktori yang berfungsi untuk menyimpan rule snort. Rule ini nantinya digunakan untuk mencocokan paket data yang masuk sehingga bisa diambil kesimpulan apakah paket data yang masuk tersebut termasuk dalam kategori serangan jaringan komputer atau bukan.

C. Integrasi SNORT dengan Acid BASE

Acid base digunakan sebagai tampilan agar hasil pembacaan snort bisa dibaca dengan mudah. Sebelum melalkukan instalasi Acid Base, terlebih dahulu diinstall barnyard2 agar hasil pembacaan snort bisa disimpan dalam mysql database.

Acid base diguat menggunakna bahasa pemrograman php dan memanfaatkan librari php adodb. Base dapat diakses melalui 192.168.56.130/base.

Base menunjukkan beberapa informasi tentang network intrussion detection system yang terpasang pada komputer server. Informasi itu adalah jumlah alert yang dibangkitkan snort, jumlah sensor, jenis alert, source IP dan destination IP.

D. Pengujian Snort IDS

Pengujian SNORT dilakukan dengan melakuakn tes pengiriman pesan menggunakan protokol ICMP dan port

scanning. Pada local rule ditamahkan rule deteksi ping dan port scanning agar snort mampu mengenali jenis serangan yang dilakukan.

SNORT mampu mendeteksi sernagan ajringan komputer yang menggunakan beberapa protokol yaitu, ICPM, UDP, TCP dan Portscan Traffic. Pada sebuah serangan dimungkinkan menggunakan beberapa protokol secara bersamaan. Pada kasus ini serangan port scanning melibatkan protokol ICMP dan TCP.

E. Pengukuran Tingkat Akurasi

Berdasarkan hasil pengujian didapatkan bahwa SNORT mampu mendeteksi semua serangan pada jaringan komputer dengan menangkap paket data dan mencocokkan dnegan database snort. Snort tidak bisa mendeteksi serangan pada jaringan komputer jika pada database snort tidak terdapat rule yang sesuai.

VI. KESIMPULAN DAN SARAN

Berdasarkan hasil yang telah dicapai pada penelitian ini, dapat disimpulkan sebagai berikut:

A. Snort IDS memudahkan administrasi jaringan dalam melakukan monitoring keamanan jaringan komputer.
B. Acid Base yang terhubung dengan Mysql database memudahkan user dalam mendapatkan informasi tentang snort IDS.
C. Konfigurasi Snort IDS dalam melakukan monitoring keamanan jaringan komputer berhasil dengan baik pada lingkungan sistem operasi Linux Ubuntu Server 14.04 LTS.

Berdasarkan hasil yang telah dicapai pada tahap penelitian ini dapat disarankan untuk melakukan konfigurasi SNORT IDS pada lingkup jaringan yang lebih luas, dimana bisa diakses dari Internet.

DAFTAR PUSTAKA

[1] Azikin, Askari. 2011. Debian GNU/Linux. Bandung: Informatika
[2] Dawson, C. W. (2009). Projects in Computing and Information Systems A Students Guide. Essex: Pearson Education Limited.
[3] O'Reilly.2009. http://commons.oreilly.com/wiki/index.php/Snort_Cookbook/Logging,_Alerts,_and_Outpu_Plug-ins#Logging_to_Email, 27 Maret 2016
[4] Sahid Aris Budiman, dkk. 2014. Implementasi Intrusion Detection System (IDS) Pada Server Debian Menggunakan Jejaring Sosial Sebagai Media Notifikasi dalam jurnal Jarkom Vol. 2 No. 1 Desember 2014
[5] Savano Miatama. 2012. Sistem Pendeteksi Serangan Menggunakan Smartphone (Tugas Akhir). Surabaya: Politeknik Elektronika Negeri Surabaya