MONITORING SERANGAN PADA JARINGAN KOMPUTER MENGGUNAKAN SNORT BERBASIS SMS GATEWAY

Abdul Aziz[1], dan Arry Budi Kurnia
Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta, Depok 16425
Email: [1]abdul.aziz@tik.pnj.ac.id

Abstract

The current rapid development of technology make network security becomes very important. Increasing number of devices connected to a network makes a lot of security gaps in the network. Administrator plays an important role in protecting the security issues on a network. The problem comes when the administrator can not always be in front of the computer to monitor the network due to illness, fatigue or are there other matters while at the same time need information fast when there is interference on the network. This problem can be solved by adding a system for the detection of traffic data or called by IDS. IDS will be linked to the SMS gateway so that the administrator can receive notification disruption on the network. In this study, researchers conducted the analysis and testing of the problems that arise so that it will produce a system that is able to detect attacks or disruptions on networks quickly and can alert the network administrator so the administrator can take precaution against disturbances more quickly. Attacks can be detected from the pattern of attacks are on the IDS rule that an intruder trying to break will be detected and the system will send SMS to the administrator.

Keywords: administrator, monitoring, network, IDS, SMS Gateway

Abstrak

Perkembangan teknologi saat ini yang cepat membuat keamanan jaringan menjadi sangat penting. Peningkatan jumlah perangkat yang terhubung ke dalam sebuah jaringan membuat banyak celah kemanan pada jaringan. Administrator berperan penting dalam melindungi masalah keamanan pada suatu jaringan. Masalah datang ketika administrator tidak bisa selalu berada di depan komputer untuk mengawasi jaringan karena sakit , kelelahan atau sedang ada urusan yang lain sementara pada waktu yang sama membutuhkan informasi yang cepat bila ada gangguan pada jaringan. Masalah ini dapat diatasi dengan menambahkan suatu sistem untuk deteksi lalu lintas data atau disebut dengan IDS. IDS akan dihubungkan dengan sms gateway sehingga administrator dapat menerima notifikasi gangguan pada jaringan. Dalam penelitian ini, peneliti melakukan analisis dan pengujian terhadap masalah yang timbul sehingga akan menghasilkan sebuah sistem yang mampu mendeteksi serangan atau gangguan pada jaringan secara cepat dan dapat memberikan peringatan kepada administrator jaringan sehingga administrator dapat mengambil langkah antisipasi terhadap gangguan lebih cepat. Serangan dapat terdeteksi dari pola serangan yang berada pada rule IDS sehingga penyusup yang mencoba masuk akan terdeteksi dan sistem akan mengirimkan sms kepada administrator.

Kata Kunci: administrator, monitoring, network, IDS, SMS Gateway

PENDAHULUAN

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak bertanggung jawab.

Sistem monitoring serangan pada jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem juga tidak memiliki interaksi dengan administrator pada saat administrator tidak sedang memantau sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis.

Selain itu sistem pertahanan terhadap aktivitas serangan saat ini umumnya dilakukan secara manual oleh administrator. Hal ini mengakibatkan

integritas sistem bergantung pada ketersediaan dan kecepatan administrator dalam merespons gangguan. Apabila terjadi serangan, administrator tidak dapat lagi mengakses sistem sehingga tidak akan dapat melakukan pemulihan sistem dengan cepat.

Oleh karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat sehingga memungkinkan administrator untuk mengetahui kapan saja dan dimana saja saat terjadi upaya penyerangan terhadap server. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan.

Dari latar belakang di atas, dapat ditarik suatu permasalahan untuk dilakukan penelitian dengan masalah Serangan pada Jaringan Komputer dan merupakan sistem yang dapat melaporkan menggunakan SMS ini, yaitu : Merancang sistem keamanan jaringan komputer yang dapat mendeteksi serangan secara otomatis dan menampilkan analisis serangan dalam bentuk web yang bisa diakses serta mengintegrasikan aplikasi yang terkait dengan sistem keamanan jaringan komputer dengan sms gateway.

Penelitian membatasi lingkup penelitian: Sistem keamanan jaringan komputer pada sistem operasi Debian 7.0, Sistem menggunakan Snort *Intrusion Detection System* yang akan dirancang dan diintegrasikan dengan SMS *Gateway*, dan pembahasan serangan pada rules IDS SNORT.

Berdasarkan perumusan masalah dan lingkup penelitian, peneliti merumuskan tujuan program dengan masalah Serangan pada Jaringan Komputer:

- Meningkatkan sistem keamanan jaringan terhadap serangan dari luar.
- Memastikan kondisi server dan jaringan tidak terganggu, tanpa harus berada di depan monitor setiap saat.
- Proses monitoring jaringan dan server dapat dilakukan kapanpun dan dimanapun.

Target luaran yang diharapkan dari penelitian ini adalah Informasi serangan terhadap server dapat dengan cepat sampai kepada administrator melalui sms gateway sehingga administrator tidak harus selalu berada di depan komputernya untuk memonitoring jaringan.

Target luaran yang lainnya diharapkan dari hasil penelitian ini, peneliti dapat mengikuti seminar nasional, dan memasukkan pada Jurnal ilmiah bidang TIK ber ISSN dan diharapkan yang terakreditasi.

Sistem ini terbagi menjadi 3 komponen utama yang bertugas untuk mengirimkan data dari *server* ke perangkat administrator melalui *sms gateway*, yaitu komponen pemantauan lalu lintas paket data (Snort), komponen pengumpulan data berdasarkan log dari snort (BASE), komponen pengiriman notifikasi berupa sms ke administrator (SMS Gateway). Kesemua komponen tersebut saling berkaitan untuk mengirimkan data yang didapat dari hasil pemantauan lalu lintas paket yang lewat pada jaringan yang kemudian didistribusikan kedalam *database* sehingga bisa diteruskan oleh *sms gateway* ke handphone administrator yang bertanggung jawab terhadap server tersebut.

Kegunaan program hasil dari penelitian kami dapat diterapkan pada permasalahan *serangan* pada Jaringan Komputer:

- Berguna untuk meningkatkan sistem keamanan jaringan terhadap serangan dari luar.
- Dapat digunakan untuk mengetahui secara akurat kondisi server dan jaringan tidak terganggu, tanpa berada di depan monitor setiap saat.
- Berguna dalam proses monitoring jaringan dan server dapat dilakukan kapanpun dan dimanapun.

Pada sistem ini OS yang digunakan merupakan OS Linux. Linux adalah duplikat Unix, *kernel*-nya ditulis oleh Linus Torvalds dan dikembangkan dengan bantuan *programmer* dan *hacker* dari seluruh dunia. Linux memiliki semua fitur

yang dimiliki oleh Unix, termasuk *multitasking*, *virtual memory*, *shared libraries*, *demand loading*, *shared copy-on-write executables*, *proper memory management* dan *TCP/IP networking*.

Dengan fitur sekelas sistem operasi komersial tersebut tidak membuat Linux menjadi mahal harganya, justru Linux dapat diperoleh secara gratis. Kalaupun ada sedikit biaya itu hanya sebagai ongkos distribusi atau pembelian cd saja.

Linux didistribusikan dibawah *GNU General Public License* yaitu suatu lisensi dimana pemilik program tetap memegang hak ciptanya tetapi orang lain dimungkinkan menyebarkan, memodifikasi atau bahkan menjual kembali program tersebut tapi dengan syarat *source code* asli harus tetap disertakan dalam distribusinya.

Apache HTTP Server, biasa disebut sebagai Apache, adalah sebuah *web server* terkemuka yang memiliki peranan penting dalam awal perkembangan *World Wide Web*. Pada tahun 2009, Apache menjadi *web server* pertama yang melebihi tonggak 100 juta situs. Apache adalah alternatif pertama dari *web server* Netscape Communications Corporation (saat ini dikenal sebagai Sun Java System Web Server), dan telah berkembang dan bersaing dengan *web server* berbasis Unix lainnya dalam hal fungsi dan performa. Mayoritas pengguna *web server* Apache menjalankan OS Linux.

Apache dikembangkan dan dikelola oleh sebuah komunitas pengembang di bawah naungan dari Apache Software Foundation. Aplikasi Apache tersedia untuk berbagai jenis sistem operasi, termasuk Unix, GNU, FreeBSD, Linux, Solaris, Novell NetWare, Mac OSX, Microsoft Windows, OS/2, TPF, dan eComStation. Dirilis di bawah Lisensi Apache, Apache mempunyai karakteristik sebagai software yang bebas dan perangkat *open source*.

Sejak April 1996 Apache menjadi *server* HTTP paling populer di World Wide Web. Pada Maret 2009 Apache melayani lebih dari 46% dari semua situs di dunia dan lebih dari 66% dari jutaan tersebut adalah web tersibuk.

MySQL adalah sistem manajemen *database* SQL yang *open source* paling popular, dikembangkan, didistribusikan, dan didukung oleh MySQL AB. MySQL AB adalah perusahaan komersil, yang didirikan oleh pengembang MySQL. Berikut adalah fondasi utama MySQL [1]:

- MySQL adalah sistem manajemen *database*
- MySQL adalah sistem manajemen *database* relasional
- Software MySQL adalah *open source Server database* MySQL sangat cepat, dapat dipercaya, dan mudah untuk digunakan:
- *Server* MySQL bekerja dalam sistem terintegrasi atau *client/server*
- *Server* MySQL digunakan oleh banyak aplikasi

PHP singkatan dari PHP Hypertext Preprocessor yaitu skrip pemrograman web yang bersifat *open source*. PHP merupakan skrip yang menyatu dengan HTML dan berada pada *server* (*server side HTML embedded scripting*). PHP adalah skrip yang digunakan untuk membuat halaman web yang dinamis.

Dinamis berarti halaman yang akan ditampilkan dibuat saat halaman itu diminta oleh *client*.Mekanisme ini menyebabkaninformasi yang diterima *client* selalu yang terbaru. Semua skrip PHP dieksekusi pada *server* dimana skrip tersebut dijalankan. Dilihat dari perkembangannya, bahasa pemrograman ini memiliki perkembangan yang sangat cepat dengan jumlah pemakai yang terus bertambah, berikut perkembangan dari PHP [2]:

1. PHP/FI

   Ini merupakan cikal bakal PHP yang sekarang. Pertama dibuat oleh Rasmus Lerdorf pada 1995, pada awalnya menamakan skrip ini dinamakan "Personal Home Page Tool" yang merupakan bahasa sederhana dari bahasa p emrograman C dimana

Personal Home Page Tool ini dapat berkomunikasi dengan *database* dan bersifat *open source*. Pada awalnya Rasmus membuat bahasa pemrograman ini bertujuan untuk menyimpan data pengunjung yang melihat biodata pada situs webnya.

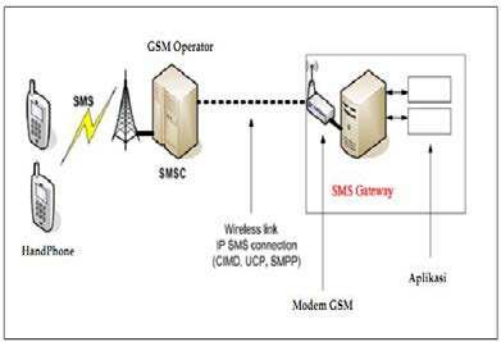
Perkembangannya, pada pertengahan tahun 1997 pemakai bahasa bahasa PHP semakin banyak, terlihat dari jumlah statistik domain yang menggunakan PHP hampir lebih dari 50.000 situs web. Kemudian karena perkembangannya yang sangat pesat, Rasmus mengembangkan bahasa pemrograman ini, dan pada bulan November 1997 muncul PHP/FI versi 2.0 yang merupakan cikal bakal PHP 3.

2. PHP Versi 3
   PHP Versi 3 merupakan versi penyempurna dari bugs-bugs pada PHP/FI versi 1.0 dan PHP/FI versi 2.0. PHP Versi 3 ini dikembangkan oleh Andi Gutmans and Zeev Suraski pada tahun 1997 yang berhasil ditulis secara sempurna pada waktu itu. Fasilitas tambahan PHP Versi 3 dibandingkan versi sebelumnya, selain tambahan fungsi-fumgsi baru, juga mendukung beberapa akses ke banyak *database*, pengelolaan protokol, dan API.
   Dari versi 3 lah singkatan PHP muncul, yaitu PHP: Hypertext Preprocessor, dan pada tahun 1998 hampir 10% situs web di dunia menggunakan PHP sebagai *webserver*-nya.
3. PHP Versi 4
   Pada musim dingin di tahun 1998, menulis ulang bahasa pemrograman PHP ini untuk membuat ketangguhan bahasa pemrograman ini. Akhirnya pada pertengahan tahun 1999 diperkenalkanlah PHP versi 4.0 yang menggunakan skrip *engine* Zend untukmeningkatkan penampilan (performa) dan mempunyai dukungan yang sangat banyak terhadap ekstensi dan berbagai *library* beserta modul. PHP versi 4.0 ini juga mempunyai keunggulan dibandingkan versi-versi sebelumnya, diantaranya mendukung ke beberapa *web server*, fasilitas HTTP session, output buffer dan sistem keamanan. Pada perkembangannya, pada saat itu hampir 20% *web server* menggunakan bahasa pemrograman PHP sebagai *interpreter*-nya.
4. PHP Versi 5
   Pada bulan Juli tahun 2005 muncul PHP versi 5.0 yang menggunakan Zend Engine 2.0 dengan penambahan beberapa fitur dan beberapa objek baru. PHP Versi 5 sangat mendukung pemrograman berbasis Object Oriented Programming (OOP).

Short Message Service atau SMS adalah sebuah layanan pada telepon genggam untuk mengirim atau menerima pesan – pesan pendek. Pada mulanya SMS dirancang sebagai bagian daripada GSM, tetapi sekarang sudah didapatkan pada jaringan bergerak lainnya termasuk jaringan UMTS. Sebuah pesan SMS maksimal terdiri dari 140 bytes, dengan kata lain sebuah pesan bisa memuat 140 karakter 8-bit, 160 karakter 7-bit atau 70 karakter 16-bit untuk bahasa Jepang, bahasa Mandarin dan Korea memakai Hanzi (Aksara Kanji/Hanja) [3].

Adapula beberapa metode untuk mengirim pesan yang lebih dari 140 bytes, tetapi seorang pengguna harus membayar lebih dari sekali.

SMS Gateway merupakan pintu gerbang bagi penyebaran Informasi dengan menggunakan SMS. SMS dapat menyebarkan pesan ke ratusan nomor secara otomatis dan cepat yang langsung terhubung dengan database nomor-nomor ponsel saja tanpa harus mengetik ratusan nomor dan pesan di ponsel karena semua nomor akan diambil secara otomatis dari database tersebut [4]. Selain itu, dengan adanya SMS Gateway kita dapat mengustomisasi pesan-pesan yang ingin dikirim.



Gambar 1. Sistem SMS Gateway

Gammu merupakan sebuah proyek yang lahir dari software untuk komunikasi dengan telepon genggam (Gnokii). Gammu sendiri memiliki kepanjangan "GNU All Mobile Management Utilities". Yang artinya gammu merupakan sofwtware utilitas untuk mengatur perangkat telepon genggam melalui PC. Awalnya gammu hanya tersedia di Linux, tetapi kini sudah ada yang tersedia untuk Windows. Gammu merupakan aplikasi console, sedang GUI nya disebut Wammu [5].

Snort merupakan salah satu contoh program NIDS yaitu program yang dapat mendeteksi penyusupan pada suatu jaringan komputer. Snort bersifat open source sehingga software ini bebas dipergunakan untuk mengamankan sistem server tanpa harus mempunyai lisence [6].

Tipe dasar IDS adalah: Rule-based system : berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mencatat lalulintas yang sesuai dengan database yang ada, maka langsung dikategorikan sebagai penyusupan [7].

Adaptive system memperguna-kan metode yang lebih canggih. Tidak hanya berdasarkan database yang ada. Tapi juga membuka kemungkinan untuk mendeteksi terhadap bentuk penyusupan yang baru.

Bentuk yang sering dipergunakan untuk komputer secara umum adalah rule-based system. Pendekatan yang dipergunakan dalam rule based system ada dua, yakni pendekatan pencegahan (preemtory) dan pendekatan reaksi (reactionary). Perbedaannya hanya masalah waktu saja. Pendekatan pencegahan, program pendeteksi penyusupan akan memperhatikan semua lalu lintas jaringan. Jika ditemukan paket yang mencurigakan, maka program akan melakukan tindakan yang perlu. Pendekatan reaksi, program pendeteksi penyusupan hanya mengamati file log. Jika ditemukan paket yang mencurigakan, program akan melakukan tindakan yang perlu. Snort dapat dioperasikan dalam 3 mode, yaitu [8]:

- Sniffer mode, untuk melihat paket yang lewat di jaringan.
- Logger mode, untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
- Intrusion Detection Mode, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini diperlukan setup dari berbagai file atau aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan. Snort mode logger pada umumnya menggunakan file untuk menulis log nya, namun snort juga menyediakan log ke dalam database mysql, freebsd maupun oracle. Dengan dukungan database maka akan memudahkan dalam proses pembacaan data log oleh program karena database sudah sangat dikenal dan dipahami. Untuk melakukan logging ke database maka dibutuhkan setting tambahan supaya snort akan otomatis logging ke dalam database.

ACID merupakan alat analisis dan pelaporan pada Snort melalui web browser. ACID bukan merupakan aplikasi secara utuh, melainkan sekumpulan skrip PHP yang bekerja sama kemudian mengumpulkan data Snort dari database, mengaturnya dalam bentuk yang sederhana pada web browser dan secara rutin memperbaharui halaman tersebut. Beberapa hal yang dapat dilakukan ACID [3]:

- Menampilkan rincian setiap alert, termasuk alamat IP sumber dan

tujuan, kerentanan yang sedang diserang.
- Menyajikan informasi dari situs-situs keamanan jaringan.
- Mengatur informasi alert yang telah terjadi dalam format dan pengelompokan yang berbeda (contoh: Protokol terkini yang digunakan, port sumber dan tujuan yang paling sering digunakan)
- Menampilkan semua informasi alert dalam format grafis
- Menampilkan alert Snort dalam kelompok yang berbeda

Functionality test bertujuan untuk menguji apakah sistem IDS ini dapatberfungsi dengan baik dan juga sesuai dengan kriteria yang diinginkan. Kriteria yang diinginkan tentu saja dapat mendeteksi ketika terdapat adanya serangan didalam jaringan maka sistem IDS akan memberikan *alerting* yang kemudian mengirimkannya ke *sms gateway* . Pada *functionality test* akan dilakukan beberapa pengujian yang menggunakan tipe serangan yang berbeda yaitu *NetworkSurveying* yang menggunakan pengujian pada [9]:

1. *IP Scan*
2. *Port Scanning*

Karena ketika ingin melakukan sebuah serangan di dalam jaringan, maka pertamakali yang akan dilakukan yaitu mencari *ip* serta *port* yang terbuka agar dapat mengetahui *ip* dan *port* apa saja yang dapat diserang. Dalam scenario *functionality test* ini dilakukan terlebih dahulu yaitu mencari *ip* dan *port* yang terbuka, jadi apabila *functionality test* ini untuk *ip* dan *port* sudah dapat diketahui, maka skenario ini sesuai dengan yang diinginkan.

IP Scan adalah suatu aplikasi yang dilakukan untuk melakukan suatu proses *scanning*/penelusuran IP pada sebuah jaringan internet. Tentu saja jaringan ini dapat berupa LAN (Local Area Network), MAN (Metropolitan Area Network), dan WAN (Wide Area Network), sehingga dengan ip scan ini dapat mengetahui adanya suatu *ip* atau *user* yang berada di dalam jaringan. Ip scan ini didapatkan dengan menggunakan sebuah *software* yang mampu mendeteksi adanya *ip* yang aktif di dalam jaringan yaitu dengan memakai *software Angry IPScanner.*

Angry IP Scanner merupakan sebuah *tools* yang digunakan untuk mencari *IP* yang hidup atau aktif dari *range IP* yang diinginkan. Selain itu *AngryIP Scanner* juga dapat melakukan pendeteksian port yang terbuka atau pun tertutup dari IP yang aktif, sehingga dengan menggunakan *software* ini dapat mencari target yang akan diserang.

Port Scan, merupakan suatu proses untuk mencari port yang terbuka pada suatu jaringan komputer. Hasil *scanning* tersebut akan didapatkan letak kelemahansistem tersebut.

METODE PENELITIAN

Penelitian ini menggunakan metodologi pendekatan penyelesaian masalah sebagai berikut :

1. Study Literature dan Pengumpulan Data dari Berbagai Sumber, yaitu mencari dan mempelajari dari sumber pustaka buku, Journal, dan sumber informasi dari internet digunakan sebagai bahan referensi yang berhubungan dengan permasalahan yang dihadapi.
2. Perancangan sistem dari hardware dan software yang digunakan.
3. Pembuatan sistem sesuai rancangan
4. Pengujian sistem
5. Evaluasi dan penyempurnaan sistem
6. Pengujian lanjutan
7. Membuat analisa dan kesimpulan dari hasil pengujian
8. Membuat laporan penelitian mengenai hasil kegiatan penelitian.

HASIL DAN PEMBAHASAN

Pengujian

Deskripsi Pengujian Sistem

Pada bagian ini akan dilakukan pengujian sistem yang sudah dibuat berdasarkan perancangan pada bab sebelumnya.

Pengujian sistem dilakukan dengan melakukan beberapa serangan dan untuk mengetahui apakah IDS dapat bekerja dengan baik. Untuk memastikan bahwa IDS telah berjalan dengan baik, maka harus dilakukan pengujian terhadap sistem. Pengujian sistem dilakukan dengan melakukan simulasi serangan dari komputer *attacker* kepada komputer *server*.

- Target Pengujian
- Pada pengujian sistem monitoring jaringan ini, hasil transmisi data dari *attacker* ke *server* diharapkan dapat menghasilkan log berupa hasil upaya serangan yang dilakukan oleh attacker yang kemudian dapat diteruskan kepada *sms gateway* sehingga administrator mendapatkan notifikasi adanya upaya serangan berupa sms.
- Peralatan Pengujian, Tabel 1 adalah peralatan penguji.

Tabel 1. Peralatan pengujian

No	Peralatan	Fungsi
1	Raspberry Pi	Penyerang (attacker)
2	Komputer *Server*	Server yang diserang
3	Modem Wavecom 3106B	Bagian dari SMS gateway
4	Switch tp-link 8 port	LAN Concentrator
5	Handphone	Penerima SMS

Prosedur Pengujian

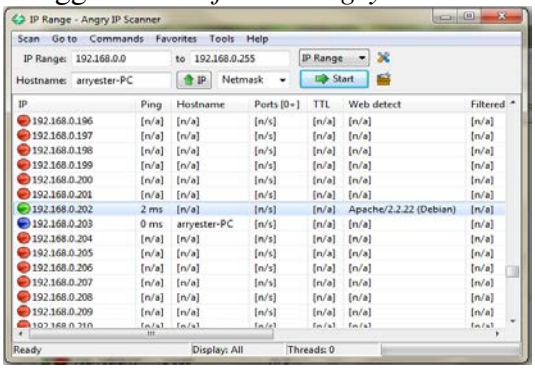
Pengujian IDS ini dilakukan dengan metode *functionality test* untuk menguji apakah sistem dapat berfungsi dengan baik dan juga memiliki tingkat *reliability* yang sesuai.

Pengujian pada penelitian ini menggunakan skenario yang dapat menganalisa data atau serangan dengan menggunakan 1 *client. Functionality Test* ini nantinya akan menguji apakah sistem IDS tersebut dapat berfungsi dengan baik yang sesuai dengan skenario yang diinginkan, untuk menghitung *response time* maka digunakan *software Wireshark. Response time* ini akan dihitung mulai dari terjadinya serangan sampai IDS memberikan respon dengan mengirimkan *alerting* kepada *sms gateway* untuk diteruskan ke administrator jaringan.

Data Hasil Pengujian

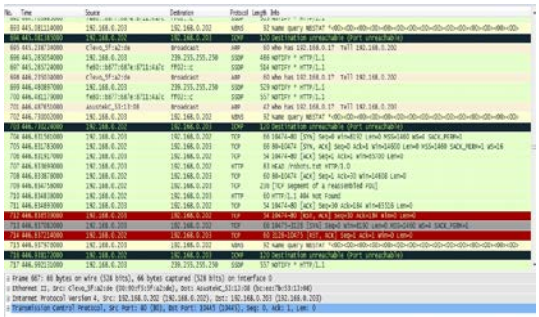
Pengujian dilakukan dengan menghubungkan dua laptop, dimana terdiri dari laptop *server* dan laptop *attacker*. Laptop *attacker* akan melakukan serangan dengan melakukan *scaning* menggunakan Angry IP. Pengujian dilakukan dengan tujuannya membuktikkan bahwa *administrator* dapat menerima notifikasi *alert* berupa sms dari serangan yang dilakukan.

Gambar 2 Hasil dari percobaan yang menggunakan *software Angry IP Scanner*



Gambar 2 Hasil dari percobaan yang menggunakan *software Angry IP Scanner*

Hasil dari Gambar 2 menerangkan bahwa *IP range* yang dipasang yaitu berkisar antara 192.168.0.0 sampai dengan 192.168.0.255. Namun gambar tersebut memperlihatkan bahwa lingkaran yang berwarna biru dan hijau adalah *IP* yang hidup atau aktif sedangkan lingkaran yang berwarna merah yaitu *IP* yang sedang tidak aktif. *IP* yang aktif tersebut yang nantinya akan dijadikan target untuk diserang. Sistem IDS ini digunakan pada komputer yang mempunyai *IP address* 192.168.0.203 yang dijadikan sebagai *attacker.* Gambar 5.2 adalah hasil tangkapan *wireshark* :



Gambar 3 Hasil *Capture* IP Scan

Hasil dari Gambar 3 tersebut menunjukan apabila menjalankan *IP Scan* yang berkisar antara 192.168.0.200 sampai dengan 192.168.0.210 maka *wireshark* dapat melakukan *monitoring* terhadap jaringan sehingga *wireshark* akan mencari paket mana saja yang akan *me-reply* dari paket ICMP, maka itu dianggap sebagai IP yang sedang hidup atau aktif. Namun apabila alamat IP yang tidak aktif maka *wireshark* akan memberi tanda dengan kata *who has.* Selain itu *IP Scan* ini dapat di deteksi oleh BASE yang memberikan *alerting* pada paket ICMP. Gambar 4 adalah hasil *capture* dan grafik dari BASE :

Gambar 4 Hasil Capture BASE

Pada Gambar 4 menjelaskan bahwa BASE mampu memperlihatkan pergerakkan *alert* yang tertangkap pada jaringan berupa grafik. Grafik ini juga menjelaskan jumlah *alert* terhadap waktu selama sistem monitoring berjalan.

Pengujian *port scan* dilakukan dengan menggunakan alamat IP Server sebagai target yaitu 192.168.0.202. Tabel 2 adalah hasil *port scanning* dengan alamat IP tujuan 192.168.0.202, protokol tcp dan keadaan/State open.

Tabel 2 Hasil Pengujian Port scanning.

Port	Service	Version
21	ftp	Vsftpd 2.3.2
22	ssh	OpenSSH 6.0p1
23	telnet	Linux Telnetd
53	domain	-
80	http	Apache 2.2.22
111	rpcbind	2-4 (RPC #100000)
10^4	http	MiniServ 1.750

Tabel 2 tersebut menjelaskan bahwa pada alamat IP 192.168.0.202 terdapat beberapa port yang terbuka, di port yang terbuka inilah mempunyai peluang untuk dapat diserang oleh penyusup. *Port Scanning* ini dapat terdeteksi pada BASE yang mampu memberikan *alerting* untuk diteruskan kepada *sms gateway* sebagai notifikasi sms yang akan dikirimkan kepada administrator. Gambar 5 adalah tampilan *alerting* dari BASE :

Gambar 5 Hasil Alerting BASE

Gambar 6 Hasil Alerting Notifikasi SMS

Pada hasil Gambar 5 menunjukkan bahwa BASE mampu mendeteksi adanya *alert* pada jaringan tersebut, ini berarti bahwa port scan merupakan serangan yang cukup berbahaya bagi jaringan sesuai dengan deteksi *alert* pada snort yang kemudian ditampilkan oleh BASE dalam bentuk tabel dan grafis.

Pada hasil Gambar 6 menunjukan notifikasi dari sms yang diterima oleh administrator jaringan atau server bahwa ada upaya untuk menyusup atau menyerang kedalam jaringan

menggunakan metode *port scanning* sehingga administrator bisa mengambil langkah antisipasi terhadap serangan tersebut.

Pembahasan

Berdasarkan hasil pengujian sistem, menunjukkan bahwa setiap serangan yang datang dari luar menuju *server* ketika Sistem IDS sedang berjalan maka Sistem IDS akan mendeteksi dan memberikan notifikasi berupa pesan singkat atau sms kepada *administrator* melalui *log* paket hasil monitoring yang terekam yang kemudian diteruskan kepada *sms gateway*.

- Sistem dapat mengidentifikasi adanya usaha-usaha penyusupan pada suatu jaringan komputer yang mempunyai kemungkinan untuk membahayakan server tersebut.
- Sistem dapat memberikan notifikasi berupa pesan singkat atau sms ke ponsel *administrator* jika ada usaha-usaha penyusupan pada suatu jaringan komputer.
- Sistem dapat memberikan informasi kepada *administrator* apabila ada penyusupan secara *realtime* sehingga *administrator* bisa dengan cepat mengambil tindakan untuk antisipasi serangan tersebut.

KESIMPULAN

Analisa dan pengujian yang telah peneliti lakukan menyimpulkan :

1. Informasi sampai kepada *administrator* melalui sms gateway sehingga *administrator* tidak harus selalu berada di depan komputernya untuk memonitoring jaringan.
2. Serangan dapat terdeteksi atau tidak tergantung pola serangan tersebut ada di dalam *rule Intrusion Detection System* atau tidak. Pengelola *Intrusion Detection System* harus mampu secara rutin mengupdate *rule* terbaru di snort.conf.
3. Untuk mempermudah analisa terhadap catatan-catatan IDS *(security event)* perlu ditambahkan modul tambahan seperti Acidbase dan dihubungkan dengan php, terbukti dengan hasil pada percobaan yang telah dilakukan.

DAFTAR PUSTAKA

[1] Kadir, Abdul, *Mudah Mempelajari Database MySQL,* Andi Publiser, Yogyakarta, 2010.

[2] Supono, *Apa Itu PHP?,* http://supono. wordpress.com/2010/09/14/apa-itu-php/, 2010, [diakses 05 Juni 2015].

[3] Anggoro, Firman, dkk, *Implementasi Laporan Deteksi Penyusupan Pada Sistem Jaringan Komputer Melalui Email Dan SMS*, Politeknik Telkom Bandung, 2010.

[4] Aji, Wahyu, *Pemanfaatan Notifikasi Sms (Short Message Service) dalam IDS(Intrusion Detection System),* Universitas Ahmad Dahlan, 2010.

[5] Ashri, Chyqen, *Pengertian Gammu, http://ashrickens.blogspot.com /2010/02/ pengertian-gammu.html*, 2010*,* [diakses 5 Juni 2015].

[6] Hartono, Puji, *Sistem Pencegahan Penyusupan pada Jaringan berbasis Snort IDS dan IPTables Firewall,* Institut Teknologi Bandung, 2011.

[7] Ariewijaya, *Optimalisasi Network Security Dengan Menkombinasikan Intrusion Detection System dan Firewall Pada Web Server,* STMIK AMIKOM Yogyakarta, 2011.

[8] Arief, Rudyanto, *Penggunaan Sistem IDS (Intrution Detection System) untuk Pengamanan Jaringan dan Komputer*, STMIK AMIKOM Yogyakarta, 2013.

[9] Information Security Breaches Survey (ISBS), *http://laporan akhir penelitian.pwc.co.uk/ auditassurance /publications/uk-information-security-breaches-survey-results-2012.jhtml*, 2012*,* [diakses 05 Juni 2015].