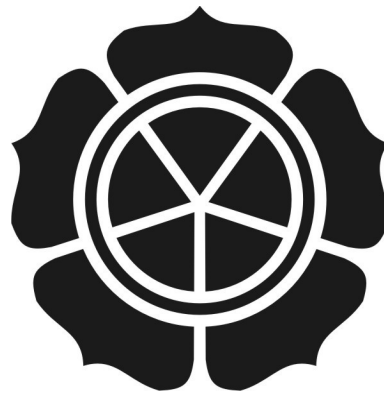


**OPTIMALISASI *NETWORK SECURITY* DENGAN MENKOMBINASIKAN
INTRUSION DETECTION SYSTEM DAN *FIREWALL*
PADA *WEB SERVER***

Naskah Publikasi



diajukan oleh

Ariewijaya

06.11.1181

kepada

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

AMIKOM

YOGYAKARTA

2011

NASKAH PUBLIKASI

**OPTIMALISASI NETWORK SECURITY DENGAN MENKOMBINASIKAN
INTRUSION DETECTION SYSTEM DAN FIREWALL
PADA WEB SERVER**

disusun oleh


Ariewijaya
06.11.1181

Dosen Pembimbing,


Melwin Syafrizal, S.Kom, M.Eng
NIK. 190302105

Tanggal, 4 Agustus 2011

Ketua Jurusan
Teknik Informatika


Ir. Abas Ali Pangera, M. Kom.
NIK. 190302008

**OPTIMIZING NETWORK SECURITY BY COMBINING
INTRUSION DETECTION SYSTEM AND FIREWALL
ON WEB SERVER**

**OPTIMALISASI NETWORK SECURITY DENGAN MENKOMBINASIKAN
INTRUSION DETECTION SYSTEM DAN FIREWALL
PADA WEB SERVER**

Ariewijaya
Jurusan Teknik Informatika
STMIK AMIKOM YOGYAKARTA

ABSTRACT

Network security is an extremely important today. The more complex and the number of computers connected together yield gaps that are vulnerable on a network. Administrator is a subject that plays an important role in protecting the web server. However, administrators have the parameters that may limited by humane limitations to protect web servers, such as, illness, limit working hours, negligence, etc.

The risk of these problems can be reduced by adding to the network infrastructure that can detect the data traffic, which is known as an Intrusion Detection System (IDS). But detection alone is not enough to make web servers secure from attack. IDS requires an automatic response, which is able to detect and prevent intrusion that come. This can be done by adding a firewall to block attacks when there are orders from IDS. In addition, the system added to the SMS gateway service that will provide information about the attack and the precautions taken.

In this thesis, the author tries to do analysis and testing on the subjects above so as to produce a system capable of detecting and protecting web servers and informative to the administrator.

Keywords: *Intrusion Detection System, firewall, SMS gateway, web server, administrators*

1. Pendahuluan

1.1 Latar Belakang Masalah

Perkembangan *website* yang semakin cepat dengan berbagai macam fungsi dan kebutuhan, menuntut meningkatnya kualitas keamanan jaringan *webserver*. Terutama dengan semakin terbukanya pengetahuan *hacking* dan *cracking*, didukung dengan banyaknya *tools* yang tersedia dengan mudah dan -kebanyakan- *free*, semakin mempermudah para *intruder* dan *attacker* untuk melakukan aksi penyusupan ataupun serangan.

Pencegahan yang paling sering dilakukan untuk masalah ini adalah dengan menempatkan seorang *administrator*. Seorang *administrator* bertugas untuk mengawasi dan melakukan tindakan *preventif* ketika terjadi aksi penyusupan dan serangan.

Masalah timbul ketika *sang administrator* sedang tidak berada pada posisi siap sedia, misalnya sakit, berada di luar jam kerja, atau adanya kepentingan mendadak. Sedangkan serangan terhadap *server* bisa terjadi kapan saja.

Maka, dari permasalahan tersebut, *administrator* membutuhkan suatu sistem yang dapat membantu mengawasi jaringan, menginformasikan serangan, dan mengambil tindakan tepat untuk pencegahan yang akan membantu mengautomatisasi fungsi kerja dasar *administrator*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas, maka dapat ditarik rumusan permasalahan sebagai berikut :

- Bagaimana membuat sistem yang dapat mengawasi lalu lintas jaringan pada *webserver* secara rutin?
- Tindakan apa yang tepat dilakukan oleh sistem dalam mengatasi berbagai macam penyusupan ataupun serangan?
- Bagaimana informasi mengenai ancaman dan serangan pada server dapat sampai dengan cepat kepada *administrator security*?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

- Membantu *administrator* dalam pengawasan jaringan server.
- Mengautomatisasi tindakan yang diambil ketika muncul gejala intrusi.
- Memberikan informasi yang tepat dan cepat mengenai serangan dan ancaman kepada *administrator*.

1.4 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini dapat dilihat dari pencapaian tujuan penelitian, yaitu :

- *Administrator* akan terbantu oleh sistem dalam pengawasan jaringan, sehingga tidak akan timbul masalah ketika *administrator* sedang lengah atau berada di luar jam kerja.
- Automatisasi tindakan yang dilakukan oleh sistem akan sangat membantu *administrator* dalam pemilihan tindakan, terutama ketika dibutuhkan tindakan yang cepat.
- Informasi yang diterima oleh *administrator* bisa menjadi bahan pertimbangan untuk perbaikan keamanan jaringan, seperti menutupi celah – celah keamanan yang *vulnerable*.

2. Landasan Teori

2.1 Keamanan Jaringan

Keamanan Jaringan menurut Dony Ariyus, dalam bukunya yang berjudul, “*Intrusion Detection System, Sistem Pendeteksi Penyusup pada Jaringan Komputer*”, adalah “Keamanan jaringan secara umum adalah komputer yang terhubung ke *network*, mempunyai ancaman keamanan lebih besar daripada komputer yang tidak terhubung kemana – mana”.

Mengetahui tujuan keamanan jaringan akan sangat membantu dalam pengembangan sistematika keamanan jaringan kedepannya. Tujuan dari keamanan komputer dapat disingkat dengan CIA, yang merupakan singkatan dari :

- Confidentiality : Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Confidentiality* biasanya berhubungan dengan informasi yang diberikan pihak lain.
- Integrity : Keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimanipulasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
- Availability : Aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan ketersediaan akses ke informasi.

2.2 Intrusion Detection System

Intrusion Detection System (disingkat IDS) 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 atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

IDS dapat didefinisikan sebagai *tool*, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktifitas jaringan komputer. Namun secara bahasa, sebenarnya nama IDS tidak sesuai dengan pengertiannya, sebab IDS tidaklah mendeteksi penyusup, melainkan hanya mendeteksi aktifitas - aktifitas pada lalu lintas jaringan yang tidak layak terjadi.

2.3 Ancaman Keamanan

Langkah awal dalam mengembangkan rencana keamanan jaringan yang efektif adalah dengan mengenali ancaman yang mungkin datang. Dalam RFC 1244, Site Security Handbook, dibedakan tiga tipe ancaman :

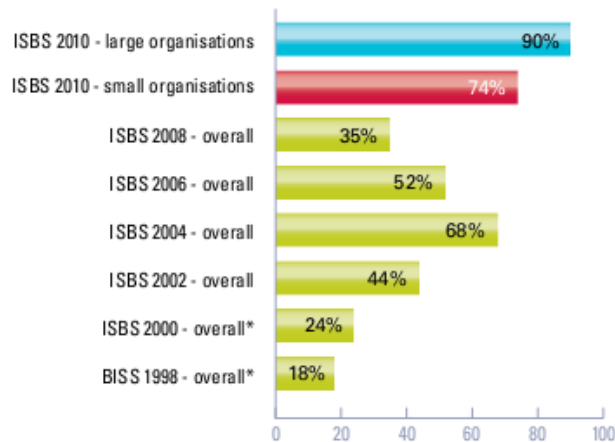
- Akses tidak sah oleh orang yang tidak mempunyai wewenang.
- Kesalahan informasi, segala masalah yang dapat menyebabkan diberikannya informasi yang penting atau sensitif kepada orang yang salah, yang seharusnya tidak boleh mendapatkan informasi tersebut.
- Penolakan terhadap *service*, segala masalah mengenai *security* yang menyebabkan sistem mengganggu pekerjaan – pekerjaan yang produktif.

3. Analisis

3.1 Analisis Masalah

Insiden – insiden keamanan jaringan dari tahun ke tahun semakin parah, fakta ini dapat dilihat dari hasil survey *Information Security Breaches Survey* (ISBS) pada tahun 2010 yang berbasis di Inggris. Grafik di bawah ini menggambarkan bagaimana insiden *malicious security* dari tahun 1998 hingga 2010¹.

¹ http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf hal.10



* The 1998 and 2000 DTI survey figures were based on the preceding two years rather than last year

Gambar 1 Grafik Serangan Tahun 1998 - 2010

3.2 Analisis Sistem

Merujuk pada analisis masalah yang dibahas pada sub bab sebelumnya, penulis telah mengidentifikasi isu – isu yang masuk ke dalam penelitian. Berikut poin – poinnya :

- Penelitian dilakukan dengan penerapan sistem *client – server*. *Client* akan bertindak melakukan aktifitas serangan yang akan di *prevent* oleh *server* yang sudah terintegrasi dengan sistem pencegahan penyusup.
- *Updating signature database* dilakukan dengan jarak interval waktu dengan *update* sebelumnya tidak terlalu jauh untuk menjaga reliabilitas dari sistem.
- Membutuhkan modul – modul pendukung yang terintegrasi untuk memberikan kebutuhan fungsional.
- Membangun tampilan *front-end* berbasis web agar manajemen *rule* dan *alert* lebih *user-friendly* .

3.3 Analisis Kebutuhan Sistem

Pembangunan sistem pencegahan penyusup ini akan membutuhkan perangkat – perangkat tertentu yang penulis bagi dalam dua kategori, yaitu kebutuhan perangkat keras (*hardware*) dan kebutuhan perangkat lunak (*software*).

3.4 Analisis Kelayakan Sistem

Studi kelayakan adalah studi yang digunakan untuk menentukan kemungkinan – kemungkinan apakah pengembangan sistem layak diteruskan atau dihentikan. Studi kelayakan merupakan kepadatan versi ringkasan dari keseluruhan analisis sistem dan proses pembuatan sistem.

Studi kelayakan menilai dari berbagai aspek – aspek penting yang berkaitan dengan penelitian ini. Mulai dari kelayakan yang bersifat teknis maupun hal – hal yang tidak berkaitan secara langsung, namun mempunyai pengaruh terhadap pembuatan sistem.

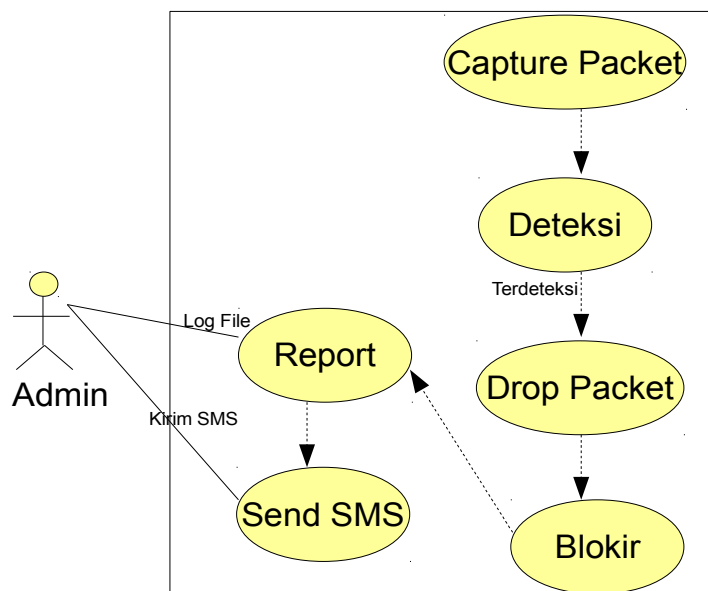
Penelitian ini menggunakan analisis kelayakan dengan melihat dari aspek kelayakan teknologi dan kelayakan hukum.

3.5 Perancangan

3.5.1 Use Case

Perancangan sistem yang digunakan untuk membangun sistem ini menggunakan UML (*Unified Modeling Language*). Perancangan dengan UML ini akan mempermudah dalam menganalisis sistem yang dibangun dengan metode OOAD (*Object-oriented Analysis and Desain*). Namun yang paling penting UML merupakan bahasa grafik (Grafical Language) yang memudahkan untuk proses perancangan sistem.

Diagram Use Case merupakan salah satu dari permodelan UML yang masuk dalam kategori Behaviour Diagram. Tujuannya menampilkan fungsi dan tugas-tugas yang bekerja di dalam sistem dan hubungannya dengan actor, yang di sini sebagai administrator.



Gambar 2 Use Case Sistem

3.5.1.1 Penjelasan Use Case

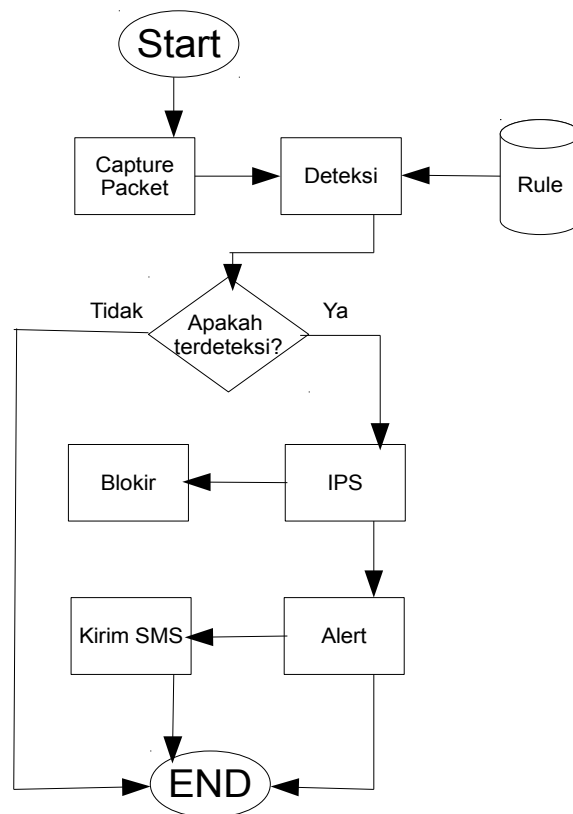
Use Case diagram yang telah digambarkan di atas merupakan tampilan kerja *Intrusion Prevention System*. Gambar tersebut menjelaskan tampilan IPS dalam menangani suatu case.

Awalnya *Packet Capture* menangkap sebuah paket dalam trafik jaringan, lalu terjadi proses pendeteksian yang akan dilakukan *Snort engine*. Setelah terjadi proses pendeteksian, apabila paket terdeteksi sebagai serangan, maka IPS akan meng *drop* paket dan melakukan blokir terhadap sumber serangan.

Setelah itu IPS akan mengirimkan laporan atau *report* yang akan disimpan di dalam *log* dan dikirim ke *administrator* melalui layanan *Short Message Service (SMS)*.

3.5.2 Diagram Alur

Diagram alur atau *flowchart* menggambarkan bagaimana jalannya sebuah sistem dalam melakukan tindak pendeteksian dan pencegahan. Berikut alur jalannya IPS :



Gambar 3 *Flowchart* Sistem

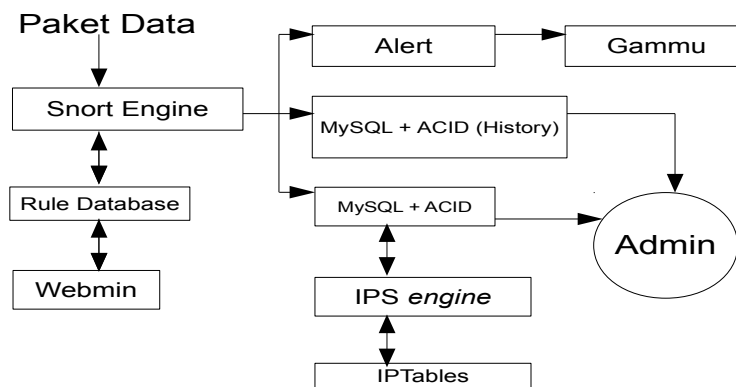
3.5.2.1 Diagram Alur

Flowchart yang ditunjukkan pada gambar di sub bab sebelumnya merupakan gambaran bagaimana proses kerja IPS secara keseluruhan. Mulanya, paket akan di *capture* lalu dideteksi oleh IDS berdasarkan *rule* yang tersedia. Kemudian apabila tidak terdeteksi maka proses berakhir, sedangkan apabila terdeteksi, maka IPS akan melakukan blokir dan mengirimkan *alert*. Lalu melalui *SMS gateway*, pesan serangan akan diterima oleh *administrator*.

3.5.3 Perancangan Hubungan Modul Sistem

Pembuatan Sistem Pendeteksi Penyusup membutuhkan modul – modul yang akan membantu IDS dan Firewall dalam melakukan pendeteksian dan pencegahan segala bentuk – bentuk serangan.

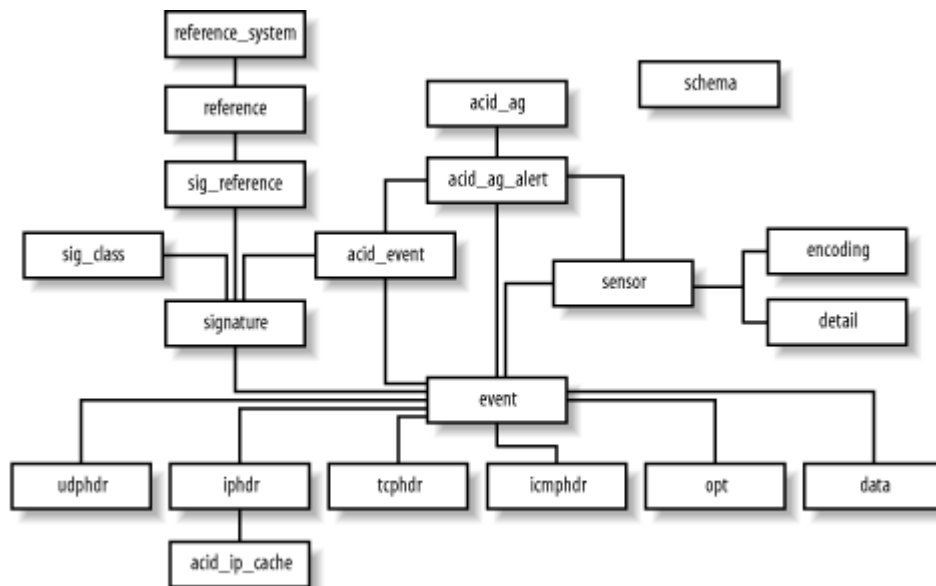
Penulis akan membuat blok diagram yang menjelaskan hubungan antara modul yang satu dengan modul yang lainnya. Berikut gambaran rancangan blok diagram IPS yang akan dibuat :



Gambar 4 Perancangan Hubungan Modul Sistem

3.5.3 Relasi Tabel Database

Penelitian ini menggunakan dua database, yaitu *database* Snort dan *database* BASE yang berikutnya akan digabung bersama dengan tabel *database* Snort. Berikut skema relasi antar tabel tersebut dan tabel Snort :



Gambar 5 Relasi antar Tabel

4. Hasil Penelitian dan Pembahasan

Pengujian dilakukan untuk membuktikan apakah *Intrusion Detection and Prevention System* mampu melindungi *webserver* atau tidak. Pengujian dilakukan sebanyak empat (4) kali dengan pengklasifikasian pengujian sebelum implementasi sistem dan pengujian setelah implementasi sistem.

Skenario pengujian dilakukan dengan menghubungkan kedua komputer dengan kabel UTP, dimana komputer *client* sebagai penyerang dan satunya sebagai komputer *server*. Komputer *client* akan mencoba melakukan serangan ke komputer *server*, dengan kondisi *server* dengan IDS yang aktif dan non-aktif. Tujuannya untuk membuktikan apakah IDS benar – benar mampu melindungi *server* atau tidak.

4.1 Scanning

Menggunakan utilitas bantu Angry IP untuk mendeteksi celah – celah keamanan, dengan mencari port – port yang terbuka pada server.

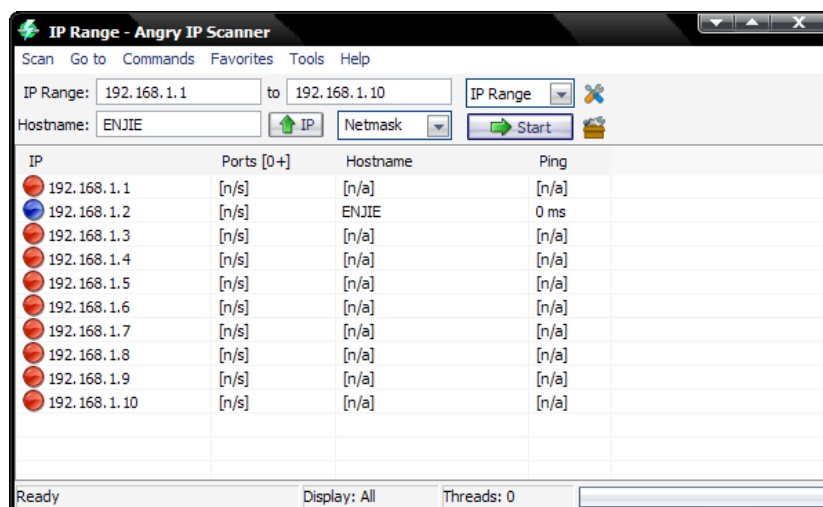
4.1.1 Reaksi Sistem

IDS mengirimkan pesan kepada *administrator* mengenai serangan yang muncul.

```
[**] [1:1808003:0] ada yang sedang scanning port yang terbuka [**]  
[Priority: 0]  
12/28-11:44:17.146195 192.168.18.10:4222 -> 192.168.18.1:1205  
TCP TTL:128 TOS:0x0 ID:51412 IpLen:20 DgmLen:48 DF  
*****S* Seq: 0x12568E16 Ack: 0x0 Win: 0xFFFF TcpLen: 28  
TCP Options (4) => MSS: 1460 NOP NOP SackOK
```

Gambar 6 Perintah Ke Administrator

Maka ketika *client* mencoba untuk melakukan *scanning* terhadap *server*, *scanning tool* tidak akan memunculkan *server* sebagai *host* yang aktif, seperti yang muncul pada tampilan di bawah ini :

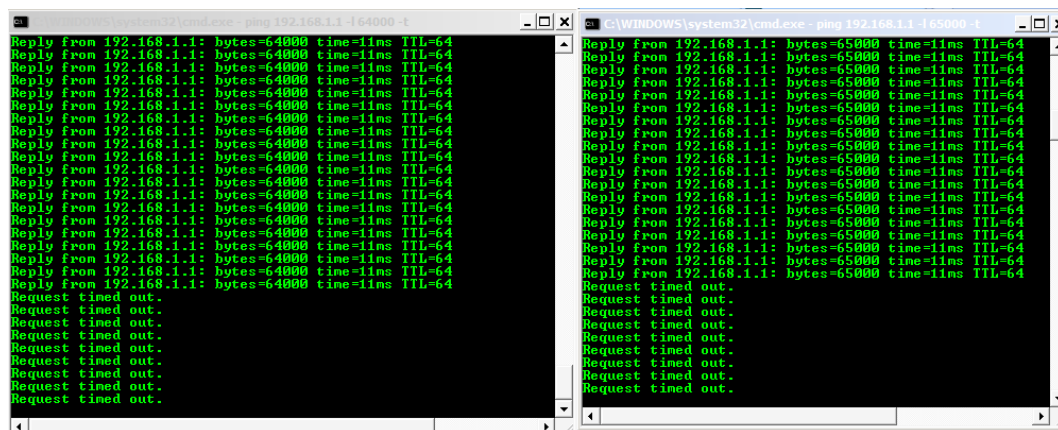


4.2 DOS Attack

Eksplotasi program ping dengan memberikan paket ICMP yang ukurannya besar ke sistem yang dituju, yaitu lebih besar dari yang diijinkan oleh protokol IP yaitu 65.536 byte. Tujuannya agar membuat sistem hang atau crash.

4.2.1 Reaksi Sistem

ketika *client* mencoba untuk melakukan *DoS Attack* terhadap *server*, program *ping* tidak akan mampu menemukan *host*, seperti yang muncul pada tampilan di bawah ini :

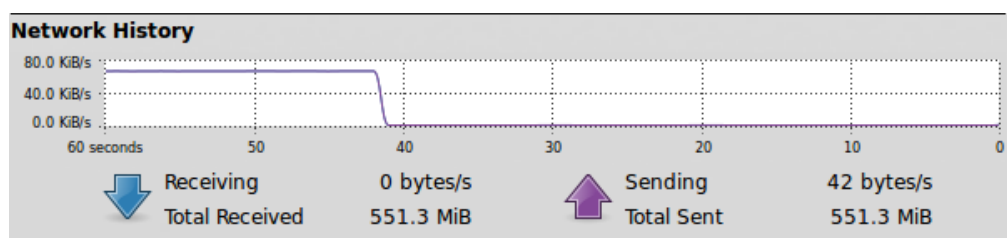


```
C:\WINDOWS\system32\cmd.exe - ping 192.168.1.1 -l 64000 -t
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=64000 time=11ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

C:\WINDOWS\system32\cmd.exe - ping 192.168.1.1 -l 65000 -t
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=11ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Gambar 8 Ping Attack Berhenti

Tindak pencegahan ini membuat trafik jaringan kembali normal. Tidak seperti sebelumnya yang menunjukkan peningkatan signifikan.



Gambar 9 Trafik Jaringan Kembali Normal

Setelah melakukan dua jenis pengujian yaitu *scanning* dan *DoS Attack*. Hasil pengujian menunjukkan bahwa setiap ada serangan yang datang dari luar menuju *host* atau *server* yang dilindungi ketika *Intrusion Prevention System* sedang berjalan, maka *Intrusion Prevention System* akan mendeteksi dan memberitahukan *administrator*, sehingga *administrator* akan memblokade IP source menggunakan *firewall*. Setelah itu *alert* yang tadi dikirimkan ke IDS akan dikirimkan juga melalui SMS gateway ke *administrator*.

5. Kesimpulan

Berdasarkan dengan hasil analisa dan penngujian yang telah dilakukan dengan adanya laporan hasil skripsi yang berjudul “Optimalisasi *Network Security* Dengan Mengkombinasikan *Intrusion Detection System* dan *Firewall* pada *Web Server*” bisa dapat diambil kesimpulan sebagai berikut :

- Keamanan pada *Webserver* dapat ditingkatkan dengan pengawasan yang rutin, sehingga ketika ada serangan atau penyusupan dapat diantisipasi dengan cepat, seperti yang telah diujikan pada BAB sebelumnya.
- Tindakan pencegahan yang dilakukan adalah dengan menganalisa paket-paket data lalu ketika ada aktifitas yang dianggap sebagai serangan, maka *firewall* akan melakukan pemblokiran terhadap *IP address* penyerang.
- Informasi dapat dengan cepat sampai kepada *administrator* melalui media *SMS Gateway*. Sehingga *administrator* dapat melakukan antisipasi dengan cepat.

Daftar Pustaka

Ariyus, Dony, 2007. *Intrusion Detection System*. Yogyakarta: ANDI

Ardhiyanto, Yudhi, "Membangun Sistem Intrusion Detection Pada Windows 2003 Server" Universitas Muhammadiyah Yogyakarta

Hartono, Puji, 2006. "Sistem Pencegahan Penyusupan pada Jaringan berbasis Snort IDS dan IPTables Firewall", Bandung.

Information Security Breaches Survey (ISBS), 2010, http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf

Moore, Nick, Juni 2009, Snort 2.8.4.1 Ubuntu 9 Installation Guide.

Poerwanto, Edy, 2004. "Tinjauan Tentang Sistem Keamanan pada Web Server Aplikasi Java Servlet" Institut Teknologi Bandung.

Scarfone, Karen dan Mell, P. 2007. Guide to Intrusion Detection and Prevention System. Gaithersburg: Departement of Commerce, USA.

Sourcefire, Inc, 2010. "Snort User Manual", www.snort.org,

Syafrizal, Melwin, 2005. Pengantar Jaringan Komputer. Yogyakarta: ANDI