ANALISIS KINERJA SISTEM PENGAMANAN JARINGAN DENGAN MENGGUNAKAN SNORT IDS DAN IP-TABLES DI AREA LABORATORIUM RDNM PT. "X"

Regina Riyantika[1] , Lita Lidyawati[2] , Zul Ramadhan[3]
1. Jurusan Teknik Elektro Institut Teknologi Nasional Bandung
2. Jurusan Teknik Elektro Institut Teknologi Nasional Bandung
3. PT. TELKOM Research and Development Center Bandung
Email : regina_riantika@yahoo.com

ABSTRAK

Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari penyusup (intruder) yang bermaksud merusak sistem pada jaringan komputer ataupun mencuri informasi penting yang ada pada suatu jaringan komputer. Perancangan ini menjaga keamanan jaringan komputer dengan cara melakukan pendeteksian serangan kemudian pencegahan dari jenis serangan Port Scanning dan Denial Of Service. Setelah semua informasi serangan telah terdeteksi oleh SNORT maka user akan mengaktifkan firewall Ip-tables untuk melakukan blocking dari IP address penyerang untuk menolak semua bentuk pengiriman data serangan,seperti yang telah terpaparkan bahwa IP address 192.168.1.100 dan IP address 192.168.1.101 terdeteksi oleh server sebagai penyerang yang menyebabkan kenaikan pada memory pada server dari 123,6 Mb menjadi 177,5 Mb dan setelah IP address intruder terblocking keadaan memory menurun menjadi 135 Mb, begitupun pada pemakaian CPU setelah dilakukan serangan keadaan server meningkat menjadi 87,6 % dari keadaan normal 57,6% dan setelah IP address intruder terblocking, keadaan server kembali normal menjadi 68,3%. Setelah dilakukan proses pendeteksian dan blocking IP address pada penyerang maka sistem jaringan komputer tersebut dikatakan aman.
Kata Kunci : SNORT IDS, IP-tables, intruder

ABSTRACT

Network Security often disturbed by a threat from intruders intending destructive systems on computer network or stealing information important that were on a computer network. This design maintain the network security by conducting detection attack then the prevention of types of seizures Port Scanning and Denial Of Service. After all information offensive was detected by SNORT then user reactivated firewall Ip-Tables to do blocking of IP address attackers to reject all forms of data transmission attack, as has been exposed that IP address 192.168.1.100 and IP address 192.168.1.101 detected by the server as an attacker who cause to rise in memory on the server of 123,6 Mb be 177,5 Mb and after IP address intruder blocked the state of memory decreased to 135 Mb, including on discharging the CPU after conducted attacks the state of server increased to 87,6 % of a normal state 57,6 % and after IP address intruder blocked, the state of the server back to normal be 68,3 %. After doing the process of detecting and blocking the IP address on the computer network system of the attackers were said to be safe.

Keyword : *SNORT IDS, IP-tables, intruder*

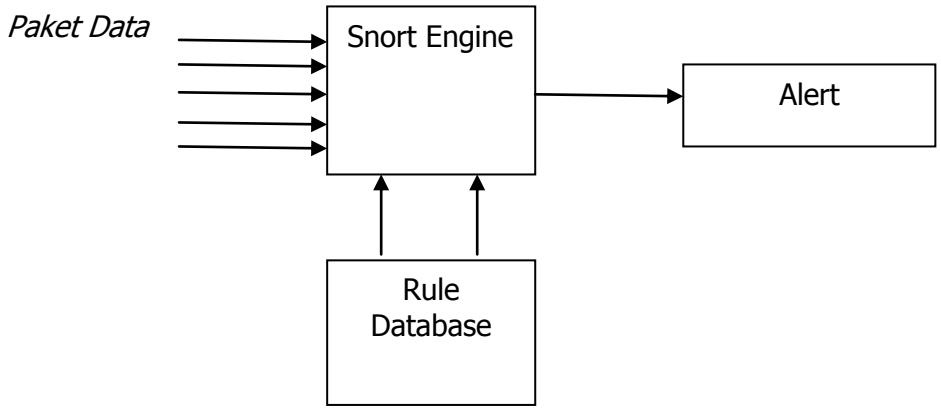
PENDAHULUAN

Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari penyusup (*intruder*) yang bermaksud merusak sistem pada jaringan komputer ataupun mencuri informasi penting yang ada pada suatu jaringan komputer (Kurniawan, 2007). Pada perancangan sistem keamanan jaringan komputer yang dilakukan adalah dengan menggunakan SNORT *Intrusion Detection System* dan *Ip-tables* untuk mendeteksi dan mencegah serangan penyusup (*intruder*) dengan menggunakan OS (*Operating System*) *LINUX UBUNTU* yang disediakan oleh layanan PT. TELKOM R&D Center, dimana memperhatikan kelayakan dan efektifitas dari penggunaan *SNORT Intrussion Detection System* serta *Ip-tables* pada area laboratorium RDNM (*Research and Development Network Management*) PT. TELKOM R&D *Center.*

Serangan DOS (*Denial Of Service attacks*) adalah jenis serangan terhadap sebuah komputer atau *server* di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut (Rafiudin, 2009).

Port Scanning merupakan ancaman yang cukup serius bagi suatu sistem jaringan komputer, dan menjadi hal yang sangat menguntungkan bagi para attacker. Dengan PORT scanning, attacker mendapatkan informasi-informasi berharga yang dibutuhkan dalam melakukan serangan. Dengan kata lain, melakukan *Port Scanning* ialah untuk mengidentifikasi *port-port* apa saja yang terbuka, dan mengenali OS (*Operating System*) target (Rafiudin, 2009).

Intrussion Detection System adalah pemberi sinyal pertama jika seseorang penyusup mencoba membobol sistem keamanan komputer (Kimin, 2010). Gambar 1 memperlihatkan paket-paket pendukung utama pendeteksian pada SNORT IDS dimana *snort engine, rule database* dan *alert* yang merupakan modul paket penting pada SNORT untuk mengeluarkan peringatan terhadap serangan yang telah terdeteksi. *Ip-tables* adalah suatu *tools* yang berfungsi sebagai alat untuk melakukan *filter* (penyaringan) terhadap (*trafic)* lalu lintas data. Dengan *Ip-tables* dapat mengatur semua lalu lintas yang ada dalam komputer, baik yang masuk ke komputer ataupun keluar dari komputer (Rehman, 2003)

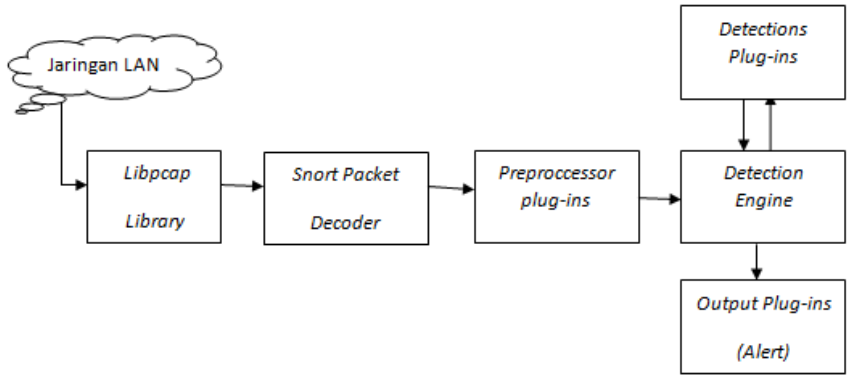


Gambar 1. Bagian pada *Intrussion Detection System* (Rehman ,2003).

2. METODOLOGI

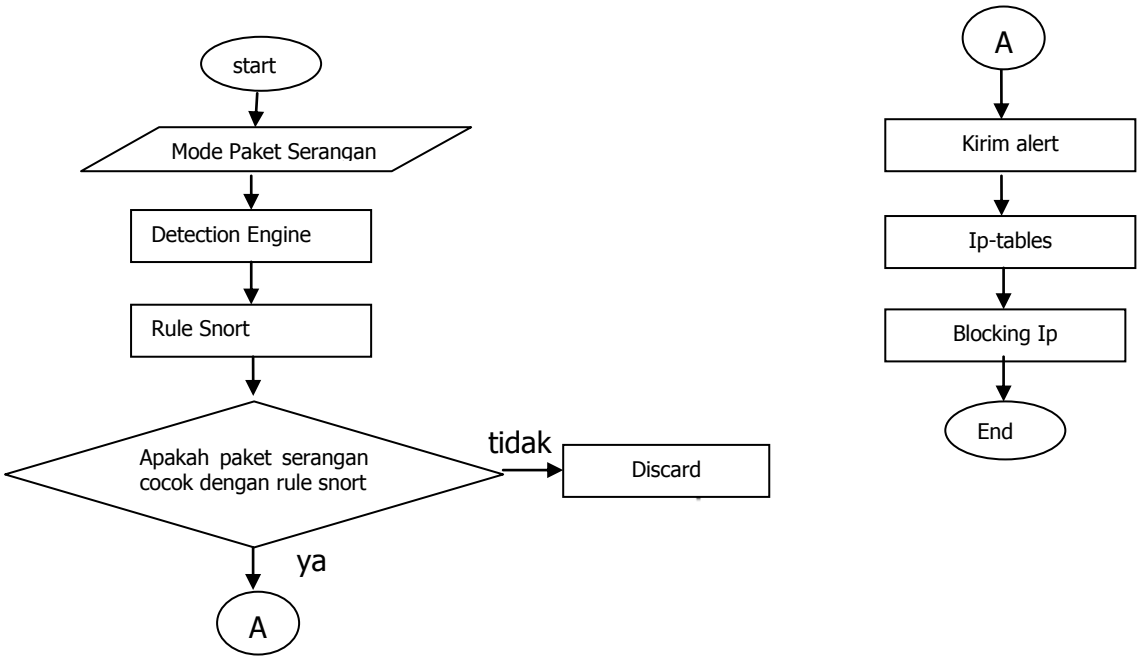
2.1 Perancangan Sistem Pendeteksian Pada Jaringan Komputer

Untuk memenuhi kebutuhan fungsional sistem pendeteksian dari penyusupan pada *SNORT Intrussion Detection System*, dibutuhkan beberapa modul-modul atau paket-paket yang harus ada dalam SNORT *Intrussion Detection System (*Ariyus, 2006). Beberapa modul-modul yang dibutuhkan itu adalah *packet decode engine, preproccessor plug-ins, detection engine, detection plug-ins dan output plug-ins (*Christine, 2006). Adapun blok diagram sistem pendeteksian pada SNORT *Intrussion Detection System* ketika ada serangan ditunjukan pada gambar 2 yang memperlihatkan paket-paket yang diperlukan pada sistem pendeteksian pada SNORT dimana *libpcap library, snort packet decoder*, dan *preproccesor plug ins* yang menangkap dan mengelompokan paket data yang ada dalam suatu jaringan, sedangkan *detection plug-ins* dan *detection engine* berfungsi sebagai sistem yang menentukan suatu paket data terdeteksi sebagai serangan atau bukan, dan *output plug-ins* yang berfungi sebagai *alert* ketika suatu paket data dinyatakan sebagai suatu serangan(Rehman, 2003).



Gambar 2. Blok Diagram Sistem Pendeteksian Pada SNORT (Rehman, 2003).

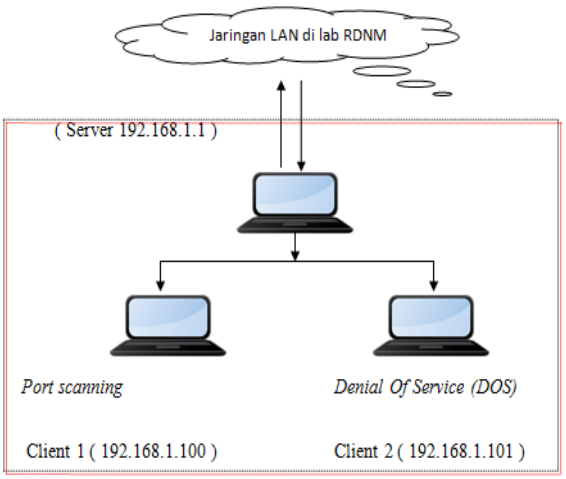
Perancangan sistem pengamanan jaringan komputer pada penelitian ini menggunakan aliran kerja (*flowchart*) terlebih dahulu agar memudahkan pembaca untuk memahami alur dari penelitian. Gambar 3 memperlihatkan urutan sistem pendeteksian pada SNORT dan pencegahan pada *Ip-tables* pada suatu jaringan yang terserang oleh serangan *Port Scanning* dan *Denial Of Service.* Diterangkan pada gambar 3 ketika sistem pendeteksian dimulai kemudian diberikan masukan paket serangan Port Scanning dan Denial Of Service ,makan akan segera diproses oleh detection engine dan rule snort, setelah itu mode paket serangan akan dicocokan dengan rule snort, apabila mode paket serangan cocok dengan rules pada SNORT maka paket data tersebut dideteksi sebagai serangan dan akan segera di proses oleh Ip-tables setelah itu akan dilakukan pemblockingan IP intruder, kemudian setelah dilakukan pemblockingan maka segala bentuk sistem pengeksploitasian data serangan terhenti.



Gambar 3. *Flowchart* Sistem Pengamanan Jaringan

2.2 Implementasi

Dalam perancangan sistem pengamanan jaringan ini topologi jaringan yang digunakan adalah sebagai berikut :



Gambar 4. Topologi Jaringan

Gambar 4 memperlihatkan spesifikasi rancangan dan topologi jaringan yang dipakai, gambar diatas menunjukan bahwa *server* bertindak sebagai komputer yang diserang oleh serangan *port scanning* dan *Denial Of Service (DOS)*, dimana serangan *port scanning* dan *Denial Of Service* dibangkitkan dari komputer *client* 1 dan komputer *client* 2.

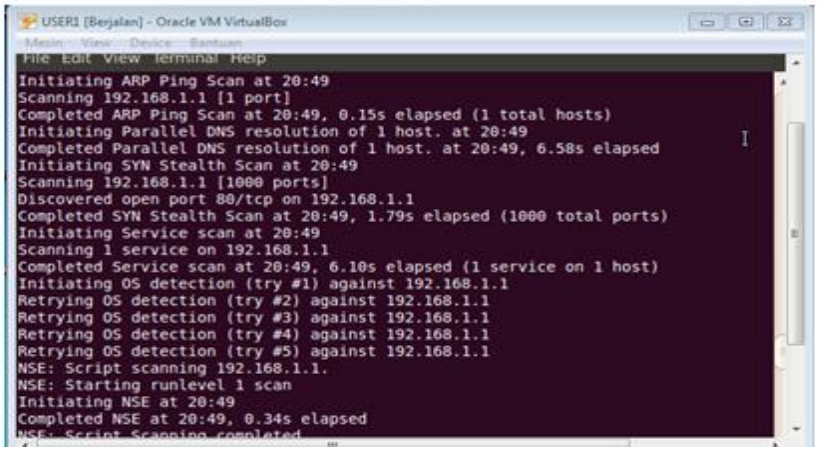
Kemudian menjalankan SNORT *Intrussion Detection System* untuk melakukan pendeteksian pada serangan yang akan dibangkitkan, dengan mengetikan perintah *server* sebagai berikut:

Menjalankan Snort :
Sudo /etc/init.d/snort start

2.3 Pengujian Rancangan

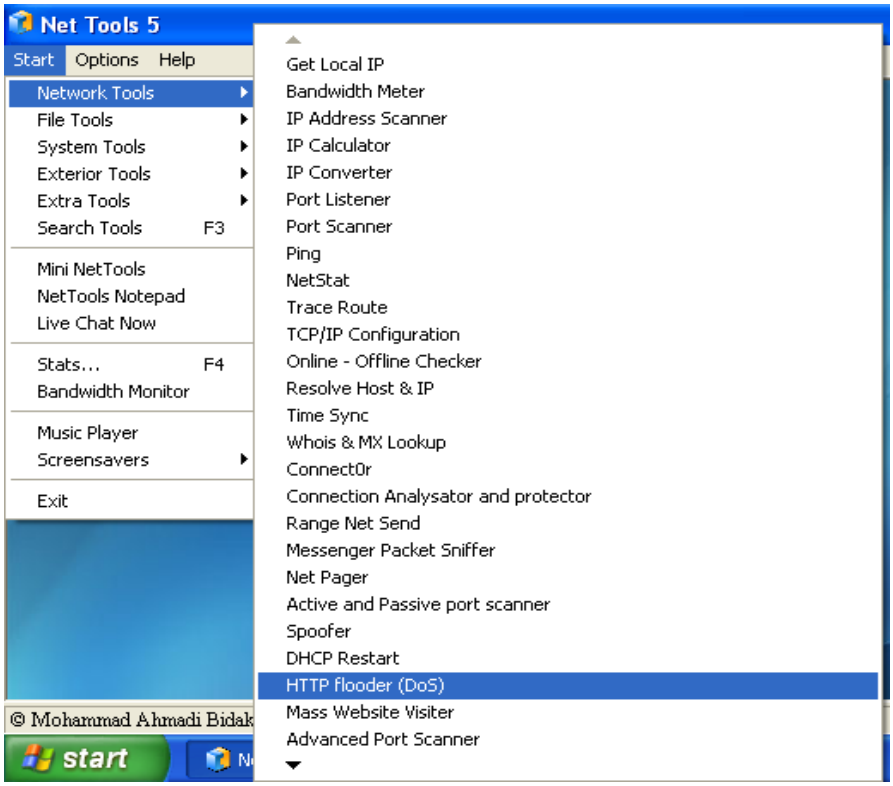
Dalam melakukan pengujian rancangan pada sistem keamanan jaringan, hal yang pertama dilakukan yaitu membangkitakan kedua jenis serangan yaitu serangan *Port Scanning* dan *Denial Of Service.*

```
#nmap –A –v 192.168.1.1
```



Gambar 5. Melakukan Paket Serangan (*Port Scanning*)

Gambar 5 memperlihatkan bahwa paket serangan *Port Scanning* pada perancangan pengamanan jaringan ini dibangkitkan oleh *Nmap* pada *client 1* dengan IP 192.168.1.100, dan pada gambar diatas menunjukan bahwa serangan port scanning telah berhasil menyerang sistem *server*.



Gambar 6. Melakukan paket serangan *Denial Of Service*

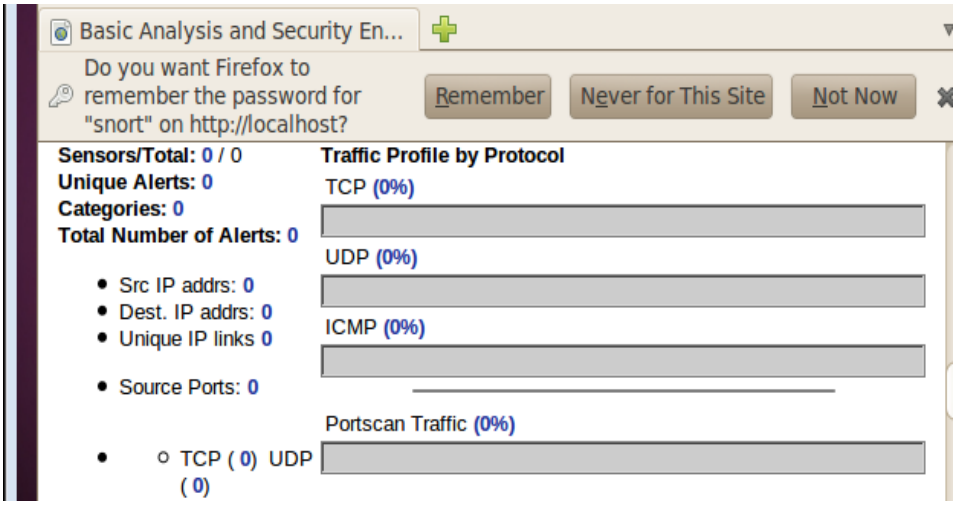
Paket serangan *Denial Of Service (DOS)* pada perancangan pengamanan jaringan ini dibangkitkan oleh *Net-Tools* pada *client* 2 dengan IP 192.168.1.101.
Gambar 6 memperlihatkan *client* 2 mengirimkan paket serangan dengan memilih menu serangan paket *flooder Denial Of Service (DOS)* pada *Net-tools* yang akan dikirimkan pada sistem *server*.

4. HASIL DAN PEMBAHASAN

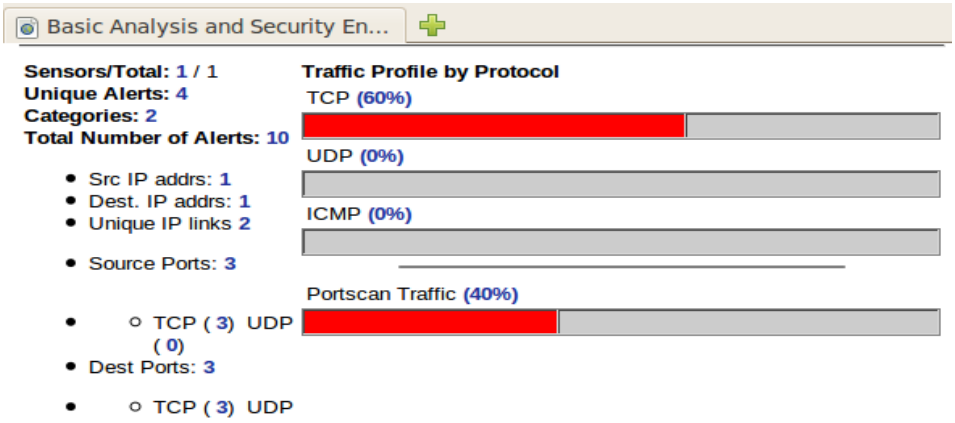
Realisasi perancangan sistem keamanan jaringan untuk mengetahui kelayakan dan kinerja dari SNORT *Intrussion Detection System* dan *Ip-tables*, parameter penting yang harus diketahui adalah data data serangan yang muncul pada *Basic Analysis Security Engine.*

3.1 Tampilan Data Serangan Pada Basic Security Engine

Untuk mengetahui semua informasi tentang serangan yang telah dibangkitkan, mulai dari IP *address* penyerang, IP *address* komputer yang diserang, waktu dilakukan serangan dan jenis serangan yang digunakan maka diperlukan aplikasi tambahan yaitu *Basic Analysis Security Engine (BASE)* agar kemudian memudahkan *user* pada *server* untuk memantau data-data serangan dan untuk melakukan pengaktifan *Ip-tables firewall* . Gambar 7 memperlihatkan tampilan *BASE* ketika keadaan sistem *server* masih dalam keadaan normal atau ketika belum ada serangan yang terdeteksi oleh SNORT

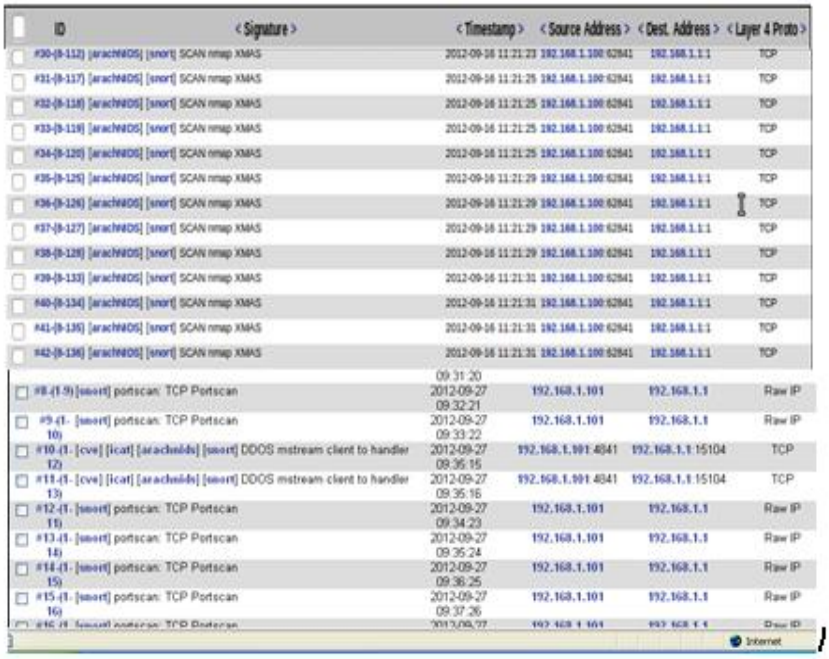


Gambar 7. Tampilan pada BASE sebelum dilakukan serangan



Gambar 8. Tampilan Pada BASE setelah dilakukan serangan

Gambar 8 memperlihatkan tampilan *BASE* ketika SNORT telah mendeteksi keadaan sistem *server* dalam keadaan terserang oleh paket serangan *Port Scanning dan Denial Of Service*. Sehingga mengakibatkan adanya perubahan pada *traffic* dalam *BASE* yaitu dengan adanya peningkatan pada nilai TCP dan *Portscan Traffic.*

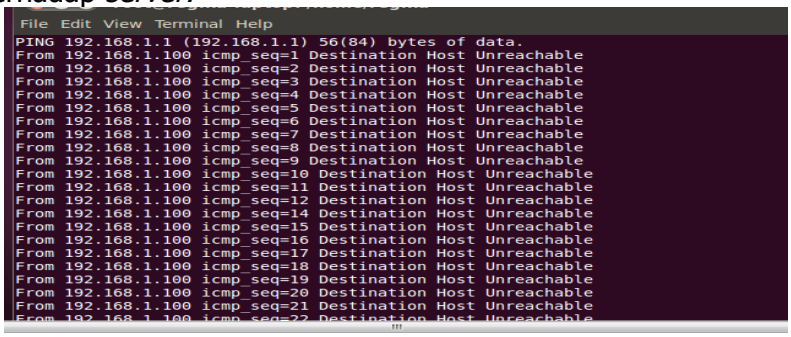


Gambar 9. Tampilan *alert* pada *BASE*

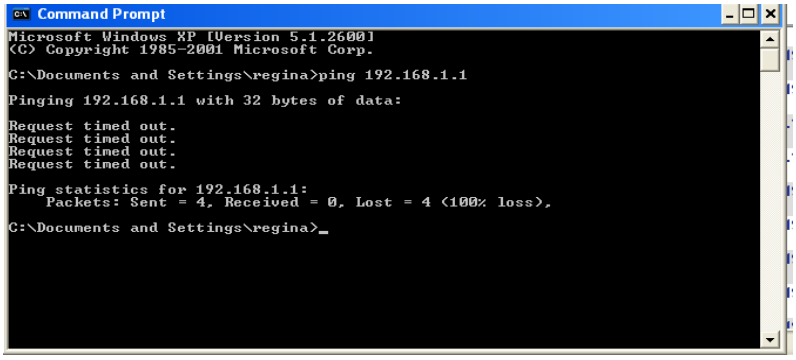
Gambar 9 memperlihatkan uraian dari data serangan pada BASE yang mencoba mengganggu kinerja sistem *server*, mulai dari IP *address* penyerang (*intruder),* IP *address* yang diserang, waktu dilakukannya serangan, serta jenis dari paket serangan.
Setelah mendapat informasi dari *SNORT* pada *BASE* bahwa adanya serangan yang dilakukan oleh *intruder* dengan *IP* 192.168.1.100 *dan IP* 192.168.1.101*,* kemudian admin pada komputer *server* akan segera memanggil fungsi *firewall Ip-tables* dengan mengetikkan perintah :

```
Iptables –A INPUT –s 192.168.1.100  -d 192.168.1.1 –j DROP
Iptables –A INPUT –s 192.168.1.101  -d 192.168.1.1 -j DROP
```

Ip-tables rules diatas menerangkan bahwa sumber paket dengan IP 192.168.1.100 dan IP 192.168.1.101 ditolak oleh sistem atau dengan kata lain IP 192.168.1.1 membuang setiap paket yang berasal dari kedua IP tersebut tanpa mengirimkan pesan ke pengirim paket. Pada gambar 10 menunjukan bahwa IP address 192.168.1.100 tidak dapat terhubung lagi kepada IP *address server* yaitu 192.168.1.1 terlihat dari balasan yang dikirimkan oleh IP *address server* yang menyebutkan bahwa IP 192.168.1.100 tidak dapat melakukan koneksi *(unreachable)* terhadap *server.*



Gambar 10. Bukti tampilan bahwa IP 192.168.1.100 tidak bisa mengakses IP 192.168.1.1

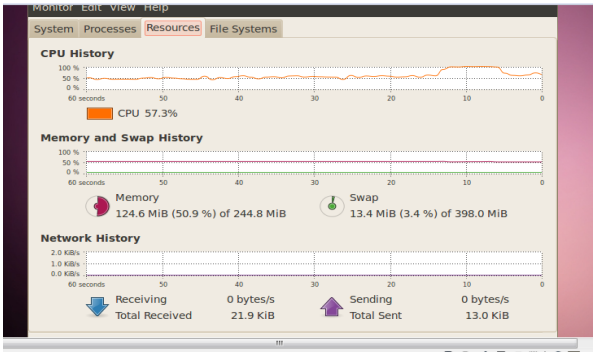


Gambar 11. Bukti Tampilan bahwa IP 192.168.1.101 tidak bisa mengakses IP 192.168.1.1

Gambar 11 memperlihatkan bahwa *intruder* sudah tidak mempunyai koneksi terhadap komputer yang diserang *(request timed out)* , sehingga eksploitasi pengiriman paket serangan pun terhenti.

3.2 Dampak Serangan Terhadap Sistem

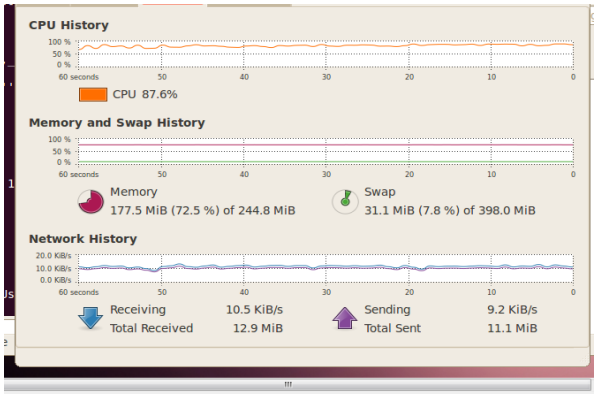
Berdasarkan hasil pengujian dari serangan yang telah dilakukan pada perancangan sistem keamanan jaringan dalam Tugas Akhir ini terlihat bahwa adanya dampak yang mengganggu sisi *performance* pada sistem kinerja *server* dapat dilihat dengan meningginya proses pada *memory, processor, swap dan traffic* pada jaringan. Gambar 12 memperlihatkan sisi *performance* pada sistem *server* ketika dalam keadaan normal yaitu ketika belum terdeteksinya serangan pada *server .*



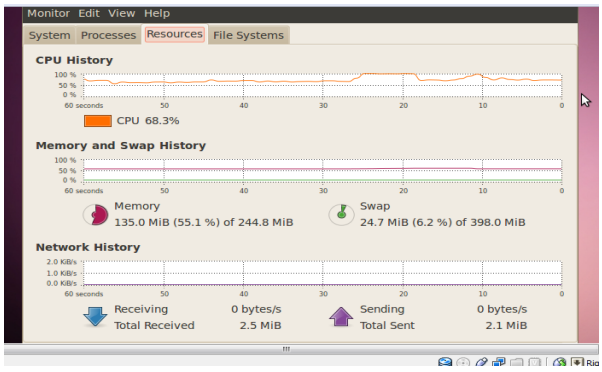
Gambar 12. Keadaan sistem *server* dalam keadaan normal (belum dilakukan serangan)

Gambar 13 memperlihatkan sisi *performance* pada sistem *server* ketika sudah dalam keadaan terserang oleh paket serangan *Port Scanning* dan *Denial Of Service*, sehingga terjadi perubahan nilai *traffic* pada *CPU history*, *Memory* dan jumlah *received* serta *sending data.*

Gambar 14 memperlihatkan sisi performance pada sistem server ketika sudah dalam keadaan terblocking oleh Ip-tables, sehingga terjadi perubahan penurunan nilai *traffic* pada CPU *history*, *Memory* dan jumlah *received* serta *sending* data, bila dibandingkan dengan keadaan terserang.



Gambar 13. Keadaan sistem *server* ketika setelah dilakukan serangan



Gambar 14. Keadaan sistem *server* ketika setelah dilakukan *blocking* menggunakan *Ip-tables*

3.3 Pembahasan

Pengiriman paket serangan yang dilakukan dalam pengujian ini adalah dengan melakukan *Port Scanning* yang dibangkitkan dengan menggunakan *Nmap d*an *Denial Of Service* yang dibangkitkan dengan menggunakan *Net-Tools. Port Scanning* merupakan jenis serangan yang digunakan untuk eksplorasi suatu jaringan komputer untuk mengetahui *port-port* mana saja yang terbuka dalam artian untuk mengetahui sistem operasi yang digunakan dan mengetahui port mana saja yang mudah untuk dilakukan serangan. *DOS (Denial Of Service)* merupakan serangan terhadap komputer atau *server* di dalam jaringan intranet dengan cara mengganggu sistem atau *resource* yang dimiliki oleh komputer tersebut sehingga tidak dapat menjalankan fungsinya dengen benar. Setelah diakukan serangan *Port Scanning dan Denial Of Service* terlihat adanya dampak yang mengganggu sisi *performance* pada sistem kinerja *server* dapat dilihat dari keadaan pada Tabel 1 yang memperlihatkan bahwa adanya perbedaan nilai *traffic* pada kinerja sistem ketika dalam keadaan normal, keadaan ketika terserang , dan keadaan setelah *terblocking*. Ketika *server* dalam keadaan terserang terjadi peningkatan nilai CPU *history*, pemakaian *memory* dan *received* serta *sending* data dari keadaan normal seperti pemakaian memory yang semula hanya 13, 4 Mb menjadi 31,1 Mb begitu pun pada history CPU yang semula hanya 57,3% menjadi 87,6% semua nilai traffic pada sisi performance mengalami peningkatan setelah dilakukan serangan, yang apabila dibiarkan akan mengakibatkan kinerja sistem menjadi lambat, *hang* atau tidak dapat berfungsi sama sekali. Namun setelah IP *adddress intruder terblocking* nilai *traffic* pada sisi *performance* menurun mendekati keadaan normal seperti misalnya pemakaian memory yang menurun menjadi 135 Mb dari keadaan 177,5 Mb begitupun nilai *traffic* pada CPU *history*

dan *received* serta *sending* data semua mengalami penurunan nilai *traffic* setelah IP *address intruder* beserta paket serangan *terblocking*.

Tabel 1. Sisi *Performance* Pada Sistem Kinerja *Server*

No	Performance System	Sebelum Serangan	Setelah Serangan	Setelah Blocking IP
1	CPU *History*	57,3 %	87,6 %	68,3 %
2	*Memory*	124,6 Mb	177,5 Mb	135 Mb
3	*SWAP Memory*	13,4 Mb	31,1 Mb	24,7 Mb
4	*Receiving* Data	0 bytes/s	10,5 Kb/s	0 bytes/s
5	*Sending* Data	0 bytes/s	9,2 Kb/s	0 bytes/s
6	Total *Received* Data	21,5 Kb	12,9 Mb	2,5 Mb
7	Total *Sent* Data	13 Kb	11,1 Mb	2,1 Mb

Paket serangan yang dibangkitkan oleh dua *Operating System* berbeda yaitu LINUX dan Windows, hasil pengujian menunjukan serangan yang dibangkitkan dengan *Operating System* LINUX lebih cepat terdeteksi dibandingkan serangan yang dibangkitkan dengan *Operating System* Windows karena LINUX memiliki keamanan yang lebih unggul daripada Windows sehingga cepat memberikan tanggapan ketika terjadi serangan dari intruder.

5. KESIMPULAN

Berdasarkan hasil dari implementasi perancangan sistem pengamanan jaringan dan analisis data yang telah dipaparkan pada bab sebelumnya, dapat ditarik kesimpulan bahwa :

1. Serangan yang dibangkitkan berhasil terdeteksi oleh *SNORT IDS* Dalam hal ini terbukti dengan adanya peringatan (*alert)* yang muncul dan memberitahukan bahwa *client 1* dengan IP *address* 192.168.1.100 dan *client 2* dengan IP *address* 192.168.1.101 mencoba melakukan serangan terhadap *server* dengan IP *address* 192.168.1.1 yang dapat terlihat pada *BASE*, semua informasi terpapar di dalamnya baik IP *address* penyerang, IP *address* sistem yang diserang, jenis serangan dan waktu dilakukan nya serangan.
2. Berdasarkan hasil pengujian dari serangan yang telah dilakukan terlihat adanya dampak yang mengganggu sisi *performance* pada sistem kinerja *server* dapat dilihat dengan meningginya proses pada memory, processor, swap dan traffic pada jaringan yaitu :
   a. *CPU history*, perubahan yang ditunjukan oleh kinerja kerja *CPU* yang melonjak menjadi 87,6 % dari keadaan normal yang hanya 57,3 %
   b. *Memory and SWAP history*, terdapat dua macam *memory* yang ada dalam LINUX yaitu *real memory* dan *virtual memory* yang dikenal dengan *SWAP.* Pada saat *intruder* (penyusup) melancarkan serangan, penggunaan *memory* meningkat dari 124,6 Mb menjadi 177,5 Mb, dan *virtual memory* yang berkurang kapasitasnya dari 384,6 Mb menjadi 366,9 Mb
   c. *Network history*, pemantau jaringan yang berhasil dipantau ketika *intruder* (penyusup) melakukan serangan, yaitu jaringan menerima 10.5 Kb paket data per detiknya, dan mengirim 9,2 Kb paket data per detik, dan dalam keadaan normal sistem hanya menerima dan mengirim 0 bytes paket data per detik. Jika keadaan ini dibiarkan dan terjadi dalam waktu yang cukup lama, maka kondisi sistem akan *hang* bahkan dapat terjadi kerusakan sistem

3. Paket serangan yang telah terdeteksi berhasil di tolak dengan adanya *Ip-tables* dalam hal ini mampu untuk memblok akses dari IP *address* penyerang yang mencoba untuk menerobos sistem server, terbukti dengan telah hilangnya koneksi antara IP 192.168.1.1 dengan IP 192.168.1.100 dan IP 192.168.1.101 jika kedua IP *address* dari *intruder* itu telah tidak terkoneksi dengan *server* maka segala bentuk *sharing* data atau pengiriman paket data tidak dapat dilakukan karena telah ditolak oleh *server*.

DAFTAR RUJUKAN

Ariyus, Dony. (2006). Membangun Intrusion Détection Pada Windows 2003 Server. Yogyakarta; Program Studi Ilmu Komputer Universitas Gadjah Mada.

Christine, Januar Ellysabeth. (2006). Aplikasi Hierarchical Clustering Pada Intrussion Detection System Berbasis Snort. Surabaya; Teknik Telekomunikasi Politeknik Elektronika Negeri Surabaya

Kimin, Ferdian Hans. (2010). Perancangan Sistem Keamanan Jaringan Komputer Berbasis SNORT Intrussion Detection System dan Ip-tables Firewall. Medan; Teknik Elektro Universitas Sumatra Utara

Kurniawan, Wiharsono. (2007). Jaringan Komputer, Andi, Yogyakarta.

Rafiudin, Rahmat.(2009). Investigasi Sumber-Sumber Kejahatan Internet, Andi, Yogyakarta.

Rehman Ur Rafeeq. (2003). Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID, Prentice Hall PTR, New Jersey.

.